IDA

INSTITUTE FOR DEFENSE ANALYSES

Independent Assessment Team Report on C2 Data

Dawn Meyerriecks
Stan Davis
Jim Pipher
Priscilla Guthrie

November 2008

IDA Paper P-4404
Log: H 08-001749

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, Task BC-1-2526, "Net-Enabled Command Capability (NECC) Program Planning and Implementation," for the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Alfred E. Brenner, Margaret E. Myers, MaryAnn Kiefer, Philip J. Walsh, Dale E. Lichtblau, John S. Crooks.

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-4404

Independent Assessment Team Report on C2 Data

Dawn Meyerriecks
Stan Davis
Jim Pipher
Priscilla Guthrie

Preface

This document was prepared by the Institute for Defense Analyses (IDA) under the Task Order, BC-1-2526, Net-Enabled Command Capability Transition. It was performed to support specific sub-tasking on implementing command and control data consistent with the Department's Net-Centric Data Strategy.

The Independent Assessment Team (IAT) members were: Ms. Dawn Meyerriecks, the technical team lead; Mr. Stan Davis; Mr. Jim Pipher; and Ms. Priscilla Guthrie. The IAT wishes to thank Mr. Hank Beebe, DISA, and Mr. Stuart Whitehead, JFCOM. Both helped define the task and worked with the IAT throughout the study providing valuable feedback, and access to documents and subject matter experts. COL Carl Porter and Mr. John Crooks, of Mr. Pontius' staff in OASD (NII), aided the IAT and the study immensely. The IAT wishes to thank the many subject matter experts who gave of their time and expertise.

The IAT also appreciated the thoughtful input from the following IDA research staff: Dr. Alfred Brenner, Ms. MaryAnn Kiefer, Dr. Dale Lichtblau, Dr. Margaret Myers, and Mr. Philip Walsh.

Contents

Figures

Executive Summary

In June 2008, the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII) established the Command and Control (C2) Data Independent Assessment Team (IAT) to review the issues surrounding C2 implementation of the Department's Net-Centric Data Strategy and to provide policy recommendations to further data sharing in support of operational requirements. Specifically, the IAT was tasked to "work the differences between the JFCOM C2 Data Standard and Core Concept and the NECC implementation of the DoD Net-Centric Data Strategy" and provide recommendations on C2 data sharing that:

- "Address the needs of the Department (not of a single program, Service or Command)
- Are optimal from a Department perspective
- Allow programs to meet their requirements within the context of the policy, with no single program driving the policy
- Support development of:
  - A policy document of less than 2 pages describing what is needed and why
  - An instruction of no more than 20 pages describing how to implement including concepts of employment."

Background. Most of the Department's current C2 applications were built using concepts and technologies developed decades ago. The acquisition processes assumed that requirements could be determined in full, early on in the acquisition process. The applications (systems) were built using classic, tightly integrated architectures, and were primarily intended for use in a rigid command hierarchy with constrained point-to-point communications. They provide common operating pictures (COPs) where predefined displays built with predetermined inputs are available to designated users, but because of the tightly integrated architectures, the displays cannot be modified to add new sources or algorithms without significant redevelopment and integration. These C2 applications are integrated application-to-application based on up-front interface requirements definition. The integration effort to negotiate, build and maintain these interfaces is time-consuming and expensive (the n-squared problem[1]). In short, the Department's current C2 applications cannot easily or readily evolve to meet changing operational requirements and the need for large-scale, global information sharing.

Advances in technology have made more flexible and expansive information technology (IT) environments possible. In 2003, the Department approved the DoD Net-Centric Data Strategy (NCDS) to take advantage of these advances and enable the vision of net-centric operations. The NCDS calls for data and services to be visible, accessible, understandable, trusted and interoperable to all authorized users on the Global Information Grid (GIG). This means

[1] Creating interfaces between all possible combinations of n nodes requires $n*(n-1)$ interfaces.

authorized GIG users should be able to publish, discover, and pull data and services of interest from any location, at any time. Users should be able to view and manipulate data using any service and toolset that enhances their understanding (e.g., on a map or in a spreadsheet, integrated with various types of sensor and reporting data) by *mashing it up*[2] with data from other services. They should also be able to *compose* processes on the fly, without requiring redevelopment or significant external integration support, for example, they should be able to substitute more effective algorithms, create more useful displays, and add new types of sensor or reporting data on an as-needed basis in the field. However, in part because the Department's enterprise IT capabilities and processes for NCDS implementation and operations are still being defined, there are many, often conflicting, approaches to implementing the NCDS.

Findings. The IAT found that data-sharing activities are occurring at multiple levels and in many organizations, but with limited success. While many government employees and contractors understand the need for data sharing, most are unclear as to specifically what is required and how it might work, let alone what it would take to transition to this new environment and architecture. Clearly, the lack of infrastructure and well-defined processes for implementation, operations, and sustainment of the enterprise data-sharing capabilities creates issues for the C2 community as it pursues the NCDS. IAT findings include:

Operations:

- C2 community activities appear to be focused on developing traditional, kinetic, Joint Task Force (JTF) C2 capabilities, while operational needs appear to be driving changes in-theater to support adaptive C2 data sharing.
- The C2 community appears more focused on development than operations, for example, the Joint Forces Command (JFCOM)-defined C2 Core lacks a run-time component.
- Operational data-sharing metrics are not collected and used to focus investments on better supporting operational needs, for example, using metrics from deployed Integrated Imagery and Intelligence (I3) to empirically determine usage patterns.

Roles and Responsibilities:

- New and inconsistent policies have created confusion, for example, for portfolio management. DoD Directive 7045.20 is new and not yet well understood. DoD Directive 8115.01 provides governance constructs not available in DoDD 7045.20, leaving areas for potential conflict.
- Roles and responsibilities with respect to C2 data sharing are not well understood, for example, as they relate to C2 Capability Portfolio Management (CPM), Communities of Interest (COIs), and program management.

---

[2] A mashup is a Web application that combines data from more than one source into a single integrated tool; an example is the use of cartographic data from Google Maps to add location information to real-estate data, thereby creating a new and distinct Web service that was not originally provided by either source (http://en.wikipedia.org/wiki/Mashup_%28web_application_hybrid%29).

Departmental Processes:

- The Department's funding process does not readily support data-sharing constructs, for example, funding is focused on individual Programs of Record (PoRs), but data-sharing services implementation and operations and collaborative COI activities require leadership involvement, and success depends on orchestrating multiple PoRs.
- Collaboration and data sharing with and among international partners are not compatible with traditional DoD processes, for example, the Multinational Interoperability Programme DoD and configuration management. The STANAG (Standardization Agreement) approval processes and DoD organizational structures are also not compatiable.

Technical Management:

- Many enterprise IT capabilities required to support data sharing do not yet exist. Well-defined plans and specifications for these data-sharing capabilities have not been developed or are immature. (Net-Enabled Command Capability (NECC) requires an information-sharing environment.)
- Technical management processes to support transition to a service-oriented architecture (SOA), where data is separated from applications and services, are in development by various organizations but do not appear to be coordinated, for example, configuration management, version control, net-centric testing and help desk support.
- The JFCOM-defined C2 Core is: 1) large and complex, 2) not easily modularized, 3) not adequately focused on run-time (operations).

Conclusions. The IAT concluded that transitioning from the current tightly integrated, brittle, PoR-focused C2 IT environment and acquisition approach to agile, mutually supportive C2 data sharing, acquisition and operations will require changes to many existing processes and that these processes will, for the most part, need to evolve over time as the new environment becomes more capable. Many of these processes will need to be more clearly defined and potential changes understood to support development of a comprehensive C2 implementation plan. However, the IAT believes policy and implementation guidance can be used effectively starting now to address and clarify existing issues and to focus attention on high priority, high payoff actions.

Recommendations. The IAT recommends the C2 community clearly state its intent to create and sustain an operationally responsive, collaborative C2 environment. To do this, the IAT recommends the C2 community:

- Establish *edge innovation* as a C2 goal, to enable: 1) operators to publish, discover, use, and manipulate data in ways that cannot be imagined a priori, and to do it dynamically in the field; and 2) rapid technical as well as operational innovation to support kinetic, non-kinetic, and combined missions with traditional and non-traditional partners. Figure 1 shows a C2 data sharing environment where operators have access to data and services anytime and anywhere and can publish, discover, use and manipulate data from existing and new sources, as required. Operators work directly with developers to innovate new data sharing capabilities as required. Developers access C2 Core capabilities available on the GIG to create the required shared information packages, including additional vocabulary and any needed mediation. Fast-paced test and evaluation (T&E) is carried out over the network with

online assistance from test centers. New data services, products and artifacts are then registered so that they can be discovered and exploited by others.

- State the expectation that the C2 community will implement the NCDS and use acquisition documentation to gauge progress.
- Collect and use metrics to assess utility and performance, measure progress and focus investments to support operational needs.

The IAT recommends the C2 community define the C2 data sharing constructs. Figure 1 shows a re-defined C2 Core. IAT recommends this re-defined C2 Core: 1) support UCore version 2.0, 2) be accessible via services (e.g., to use the model and vocabulary), 3) leverage the JFCOM-defined C2 Core to the extent practical, and 4) be implemented incrementally, prioritizing operationally useful increments.

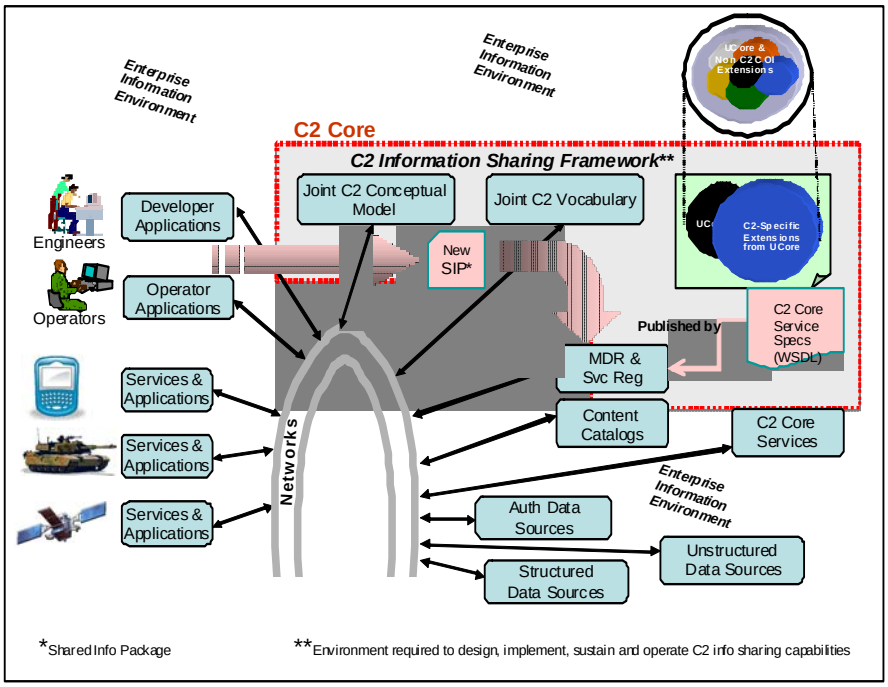

Figure 1. C2 Data Sharing Environments to Support Edge Innovation

The recommended C2 Core components are:

- *Joint C2 Conceptual Model and Vocabulary*: Model and vocabulary, used via services, which publish descriptions of C2 entities and their interrelationships together with terms and definitions that express properties of those entities.
- C2-*Specific Extensions from the UCore*: Schema components and vocabulary added to the UCore as required, providing an ability to share more detailed data within the C2 community. C2-Specific Extensions from UCore are under configuration management of the C2 CPM in cooperation with the C2 community.
- *C2 Core Service Specifications*: Specifications for cooperating C2 mission services that perform functions required to support command and control of operations.

- *C2 Information Sharing Framework (C2ISF)*: A run-time environment that enables data sharing for C2. This environment exploits DoD enterprise information environment capabilities to provide required registries (service, metadata), content catalogs, access control arrangements, mediators, crawlers and tagging engines, development and test tool kits, and instrumentation to provide user feedback, and metrics collection.

Roles and responsibilities with respect to data need to be clarified for the C2 community. While there are issues with respect to roles and responsibilities outside the community, creating a C2 baseline and using it to engage other stakeholders in the required dialog will be helpful. The IAT recommends the C2 community issue policy guidance on organizational roles and responsibilities with respect to C2 data as follows:

- OASD (NII)/DoD CIO – Establish and maintain C2 data sharing policies and framework, review acquisition documentation and metrics to assess progress, scale delegated authorities based on operational metrics, use results to focus resources.
- C2 CPM – Define, orchestrate, and maintain the C2 Core; maintain and publish operational requirements based on metrics; prioritize data-sharing efforts; publish and maintain transitional interoperability tracking devices; coordinate with other portfolios; define forecast and report operational metrics; coordinate CM and test; support and track COIs and manage artifacts; define core lifecycle management processes and assign roles and responsibilities.
- Joint Staff – Review and, as necessary, revise processes for managing existing message standards.
- Combatant Command (COCOM)/Services/Agencies – Share operational metrics; publish priorities and needs; participate in service development and integration.
- Component Program Executive Officers (PEOs)/Program Managers (PMs) – Provision, operate and use the C2 Core to implement the NCDS; participate in COIs; use scalable, interoperable data stores; participate in CM processes; define and use data usage metrics; publish and maintain interoperability tracking devices.
- Infrastructure Providers – Orchestrate distributed CM; publish information-sharing development status and metrics; develop and operate required data-sharing infrastructure services; actively participate in data-sharing service/product development and integration; provide a robust metadata environment including federation.

Today, there are in-theater examples of our forces' inability to access and to share data generated by and for the C2 community because of the tightly integrated, point-to-point architecture. Yet, in multiple instances warfighters have found ways to share data and to collaborate using a wide variety of workarounds. The IAT believes the C2 community's transition from point-to-point to a data-sharing environment will be difficult, but it is achievable; the need for and viability of this approach is being demonstrated in current operations. The IAT's strongest recommendation is for the C2 community, using this report as a basis, to immediately develop and implement an operationally focused plan to incrementally deliver these capabilities to our forces now rather than later.

1. Problem and Approach

1.1 Problem

Command and control (C2) information technology (IT) environments exist to enable better decision making by: providing timely, accurate situational awareness; supporting development of alternative courses of action and implementation of the selected course of action; and, full circle, continually updating data for timely, accurate situational awareness.

Current DoD C2 applications were built using acquisition processes that assumed requirements could be determined in full, early on in the acquisition process. They are based on classic, tightly integrated architectures. Existing C2 applications were built primarily for use in command centers, from national down to battalion, ship, and squadron levels, ashore, afloat and airborne. They feature COPs (common operating pictures) where predefined displays, with predetermined inputs, are available to all users, but cannot be modified without significant effort. These C2 applications communicate point-to-point, where the points are predetermined, based on up-front interface requirements definition. The integration effort required to negotiate, build and maintain these interfaces is time-consuming and expensive (the n-squared problem[3]). In short, the Department's current C2 applications cannot easily or readily evolve to meet changing circumstances.

The Department has a vision of net-centric operations (NCO) enabled, in part, by a Net-Centric Data Strategy (NCDS) that calls for data, including services, to be visible, accessible, understandable, trusted and interoperable to all authorized users on the Global Information Grid (GIG). Recent advances in technology have made this vision achievable. This means GIG users should be able to publish or discover and pull data of interest from any location, at any time. They should be able to view data using any service that enhances their understanding (e.g., on a map, integrated with various types of sensor and reporting data) by *mashing it up*[4] with data provided by other services. They should also be able to *compose* data-centric processes on the fly, without requiring redevelopment or extensive external integration support. For example, they should be

---

[3] Creating interfaces between all possible combinations of *n* nodes requires *n**(*n*-1)/2 interfaces.

[4] A mashup is a Web application that combines data from more than one source into a single integrated tool; an example is the use of cartographic data from Google Maps to add location information to real-estate data, thereby creating a new and distinct Web service that was not originally provided by either source (http://en.wikipedia.org/wiki/Mashup_%28web_application_hybrid%29).

able to substitute more effective algorithms, create more useful displays, and add new types of sensor or reporting data on an as needed basis in the field.

However, the Department currently has multiple, possibly conflicting or inconsistent, approaches to realizing the DoD data strategy.

1.2 Approach

The IAT used the following approach to develop the requested policy and implementation recommendations:

- Created a team with the requisite technical and operational experience in C2, IT and enterprise data
- Met with key government personnel to review the task and objectives and refine the approach, assumptions and deliverables
- Reviewed existing documentation (authoritative documents, briefs, spreadsheets, drafts, etc.)
- Met with selected subject matter experts (SMEs) to gain a thorough understanding of their perspectives (Baseline Technical Questions for these exchanges are in Appendix B)
- Documented their observations
- Used the observations to develop findings and recommendations
- Reviewed, with SMEs and stakeholders, the findings and recommendations to refine and clarify them
- Developed this report.

2. Findings

The IAT reviewed various existing artifacts (authoritative and informal), met with government stakeholders, and held detailed technical discussions with SMEs. During this process, the IAT captured and documented a number of observations. While many of these were specific to C2, the IAT also captured insights on work that must be accomplished by others to enable the vision of *edge innovation*. The IAT subsequently distilled the C2 observations and used them as the basis for five findings. This section describes each of the findings and the supporting observations. The IAT's five key C2 findings are:

1. ***Data sharing is key to force agility.***
2. ***UCore and a re-defined C2 Core could enable community-wide data sharing.***
3. ***An evolving C2 Conceptual Model and Common Vocabulary partially address data sharing needs.***
4. ***Leadership and new processes are needed to make C2 operationally responsive.***
5. ***Consistent policies are required, including strong linkages between acquisition and operations.***.

2.1 Finding 1: Data Sharing Is Key to Force Agility

Force agility depends on the ability to rapidly share and combine information in a variety of formats and media and in unplanned and innovative ways.

IAT observations:

- The battlefield is dynamic; participants, behaviors and relationships are constantly shifting, not always predictably.
- Non-governmental organizations (NGOs) and loosely coupled coalition partners are often primary players in the mission space.
- Social and cultural factors are often as important as geographical and materiel factors in situational awareness.
- Missions evolve quickly (e.g., Operation Iraqi Freedom went from conventional war to stability operations to counterinsurgency).
- Commanders need to be able to reconfigure information sources and processes *on the fly* to maintain situational awareness.
- Information and the supporting IT are key parts of the weapon suite.

- Traditional systems with embedded data have sustainment tails that are not responsive to the current operational environment.
- Data and services for discovery, access, understanding, and use must be available in theater.

Finding 1 is based on observations that should be obvious to those familiar with contemporary military operations. The IAT captured the observations for two reasons: first, because they establish baseline requirements that are significantly different from those that influenced the Department's existing C2 applications, and second, to note that the responsiveness of the Department's acquisition and development environment impacts operational agility.

2.2 Finding 2: UCore and a Re-defined C2 Core Could Enable Community-Wide Data Sharing

C2 could leverage UCore and a C2 Core consisting of: 1) a C2 Information Sharing Framework to support C2 IT development and operations; 2) a Joint C2 Conceptual Model and Joint C2 Vocabulary to provide context and the current C2 vocabulary; 3) C2-Specific Extensions from UCore to facilitate data sharing within the C2 community; and 4) C2 Core Service Specifications for C2-specific services.

The IAT had the following observations:

- Data sharing process and artifact definitions, along with associated concepts, are ill defined, leading to miscommunications and limited progress in addressing NCDS goals within the C2 community.
- The current Joint Forces Command (JFCOM)-defined C2 Core is insufficiently scoped to achieve NCDS goals and lacks operational focus.
- A number of necessary components for an operationally focused set of data and data services to support C2 exist, but are disjointed and incomplete. These include:
  - UCore (Version 2.0)
  - Metadata Registry (MDR)
  - JFCOM-defined C2 Core vocabulary (to be modified by UCore)
  - DoD Discovery Metadata Specification (DDMS)
- The C2 community has actual consumption experience with several data service offerings (e.g., Integrated Imagery and Intelligence (I3)), but there are no concerted community efforts to define the run-time data services to support C2 that are required by every command.
- Community of Interest (COI) and program management activities have identified gaps in proffered data and data services to support C2 requirements.

There is no concerted community effort to define a core set of physical data services required by, or common to, C2 operations. Most of the current focus seems to be on the development environment, with little attention to operations, including data sharing activities in theater.

2.3 Finding 3: An Evolving C2 Conceptual Model and Common Vocabulary Partially Address C2 Data Sharing Needs

The Joint C2 Conceptual Model and Joint C2 Vocabulary are published concepts that describe C2 entities and their relationships. These can be used in creating C2 extensions from UCore in conjunction with real-world operational needs, JC3IEDM artifacts, artifacts from ongoing data exchange development, and legacy message formats.

The IAT found that although the current JFCOM-defined C2 Core provides one source of vocabularies:

- It needs to be supplemented and validated against other sources (programs in development, message sets in use, etc.).
- Documented vocabularies need to be offered as part of an online vocabulary service.
- The MDR and the DoD Information Technology Standards and Profile Registry (DISR) are two existing resources that could be used to publish vocabulary standards.

The IAT found considerable confusion about conceptual models, message standards, formats for files that publish content, and physical data base schemas. They also found a variety of ways of describing the various components of requirements determination, portfolio evaluation, service analysis and design, storage management, data transformation and mediation, and fusion of data sets.

Without doubt, the most contentious issue was how to deal with the JFCOM-defined C2 Core. Some SMEs pointed to its JC3IEDM lineage – an enterprise data model with a long history, acceptance by the Multilateral Interoperability Programme (MIP), and its use in a number of European C2 environments ─ and they suggested that it should be mandated as a standard. Others were skeptical, and saw no relevancy. The IAT observed that, although the JFCOM-defined C2 Core has a number of virtues, it suffers from a number of deficiencies, including:

- It is insufficiently scoped, reflecting only joint task force (JTF)-level C2.
- The JFCOM-defined C2 Core has no run-time component, nor does it lend itself easily to a definition, or set of definitions, for run-time.
- The JFCOM-defined C2 Core is written in Unified Modeling Language (UML), which wasn't designed to capture semantics.

- The underlying model is complex. Services to aid use and interpretation are needed.
- The JFCOM-defined C2 Core is not easily segmented; subsets can involve large chunks of the model.

A C2 Conceptual Model and C2 Vocabulary are of value if and only if they are:

- Provided through net-centric services supporting transparency and accessibility for both development and operational use.
- Maintained though an online process that is sufficiently agile to respond rapidly to emergent requirements from the various global operational settings.

2.4 Finding 4: Leadership and New Processes Are Needed to Make C2 Operationally Responsive

***Moving forward requires C2 CPM leadership; defined, supported processes; infrastructure (the information environment); implementable, testable artifacts; and resources (out of the scope* of this document).**

The IAT had the following observations:

- The role of the C2 CPM is confusing; DoD Directive 7045.20 is new and not yet well understood. DoD Directive 8115.01 provides governance constructs not available in DoDD 7045.20, leaving areas for potential conflict.
- The Joint Capabilities Integration and Development System (JCIDS) and the associated Universal Joint Task Lists (UJTLs) have been analyzed to define common operations process needs and detailed data and service needs for a symmetric, JTF kinetic fight.
- The IT provisioning chain continues to be fractured along functional responsibility lines, resulting in a lack of common vision and decision criteria among key contributors.
- The C2 community is not taking advantage of operational use data in any consistent manner.
- Mandates for compliance and conformance with respect to C2 data sharing are insufficiently specific to assure NCDS goals are achieved.
- There is no overarching C2 data sharing structure to capture and take advantage of the COIs other than registration of metadata products (if any) in the MDR.
- There is a lack of understanding that CM must span the complete data and services life cycle, from needs definition through operational run-time, and that these CM processes must support on-going change as C2 evolves to support operational needs.

- Current funding processes are not matched to net-centric environments. The goal is to have the C2 community re-use data and services, as needed, but current funding processes don't reward unplanned IT behaviors. There are interesting lessons learned on this from the commercial sector.
- Planned enterprise IT capabilities to support development (e.g., the Federated Development and Certification Environment) and operations (e.g., security services, enterprise data services, MetaData Environment) are not available.

The Department has a strategy for data sharing documented in the 2003 NCDS and is in the process of moving from a tightly integrated architecture, to a net-centric, service-oriented architecture (SOA)-based environment that enables data sharing and collaboration among authorized users anywhere and any time. However, implementation of the planned enterprise enablers has been slower than planned and appears to have impacted both planning and progress in implementing C2 data sharing.

2.5 Finding 5: Consistent Policies Are Required, Including Strong Linkages between Acquisition and Operations

Policy must be consistent across multiple levels, including Department, community/mission and program, with clear goals and priorities.

IAT observations:

- C2 discussions are conflating a number of related, but different, concepts (e.g., DoD-wide C2, JTF-level C2, NECC, COIs).
- Policies and their implementations are conflicting and confusing (e.g., portfolio management).
- Goals and priorities with respect to data within the C2 community are not clear and are not obviously aligned with the DoD NCDS.

The IAT found varying levels of understanding within the C2 community of how the NCDS is being implemented. To some extent, this can be attributed to the absence of a clearly articulated plan for providing the essential enterprise capabilities required to support the NCDS. The advances in relevant information technologies (e.g., SOA, net-centricity, metadata standards, registries/directories/catalogs, services) and the changing terminology further complicate communications.

3. Policy Recommendations

The following policy considerations and recommendations address NCDS implementing actions in the C2 Capability Portfolio. They constitute potential content for the documents referenced in the IAT's task (i.e., the two-page policy document describing what is needed and why and the approximately 20-page instruction describing implementation including concepts of employment).

The IAT recommends use of policy to emphasize overarching constructs to focus and gauge the effectiveness of implementation actions. These constructs include:

1. Establish *edge innovation* as a key goal.
    - Create and sustain a data environment that implements NCDS concepts for the C2 community.
    - Enable operators to discover, use and manipulate data in ways that cannot be imagined a priori and to do so dynamically while deployed.
    - Enable collaborative, integrated operational and technical innovation that melds development and operations assets in support of kinetic, non-kinetic, and combined missions with traditional and non-traditional partners.
    - Recognize the requirement for data mediation, which represents a large and increasing percentage of the DoD IT investment. Connect ongoing mediation activities via transparent, collaborative processes (and capabilities) to fast-track warrior requests for data sharing.
2. Emphasize the importance of metrics.
    - Continually collect empirical data and metadata usage metrics from developmental, pilot and operational C2 environments.
    - Use "hard" metrics and user feedback to assess utility and performance, measure progress and to steer investments.
3. Define C2-specific interoperability constructs.
    - Publish prioritized C2-specific interoperability and data sharing needs, expressed in unambiguous formats, broadly and immediately when identified in operational settings.
    - Unambiguously define, continuously measure and publish operational C2 data sharing success metrics.
    - Continually track and publish the changing C2 and key C2-related data and service versions with emphasis on highlighting tested interoperability and interoperability shortfalls.

- Represent and advocate within the C2 community for cross-COI, cross-security domain and cross-portfolio needs.

4. Clearly delineate roles and responsibilities of the following (see Appendix C for further information):
   - Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII)/DoD Chief Information Officer (CIO)
   - C2 CPM
   - Joint Staff
   - Combatant Command (COCOM)/Services/Agency operators and organic developers
   - Component program executive officers (PEOs), program managers (PMs) and non-traditional acquisition managers
   - Infrastructure providers

3.1 Policy Recommendations for ASD (NII)

Given the rapidly changing environment in which the Department must operate, the Department's expectation that information will be available to, and collaboration possible among, authorized forces anywhere and anytime, and the relatively recent availability of technology to make this feasible, it is clear that the C2 IT environment must also change, and that information should be a driver. Department policies establish the C2 environment, and the ASD (NII), as the Principal Staff Assistant (PSA) for C2, is responsible for the development and maintenance of C2 policies. This section provides data-specific policy recommendations to implement the NCDS for the C2 environment, making data visible, accessible, understandable, trusted, and interoperable across the enterprise to support superior, timely decision-making:

- Develop, publish and maintain policy to implement the NCDS as part of C2 policy: initially through a policy memo and subsequently via an update to DoD Directive 5100.30.
- Advocate use of UCore for C2 and aggressively monitor its quality, utility and responsiveness to operational requirements.
- Define the C2 data sharing environment, including C2 Core (see Section 4.0), stating that it is expected to change to support operational requirements for data sharing.
- Highlight current acquisition policy ties to data needs through the DoD 5000 series and DoD Instruction 4630.8 with regard to the Information Support Plan (ISP).
- Define and implement, or direct implementation of, governance and processes to support C2 data sharing activities.

- Specify roles and responsibilities specific to C2 data sharing and state the applicability of policy to Component PEO/PMs and to legacy and new programs of record (PoR).
- Develop, publish and maintain a C2 Implementation Strategy focused on providing direction for implementing C2 data sharing (see Section 4.0, Implementation Guidance Recommendations).
- Engage DoD CIO and Department infrastructure providers to develop a plan for the C2 Information Sharing Framework in the context of the changing DoD enterprise information environment.
- Guide C2 CPM development of data implementation processes.
- Emphasize the importance of COIs in achieving net-centricity and the role of PoR in using COIs to create workable C2-Specific Extensions from UCore. Every PoR should be registered as a participant in at least one and probably multiple COIs.

IAT recommendations on implementation are contained in Section 4.0, Implementation Guidance Recommendations.

3.2 Policy Directions to Component PEOs/PMs

As the primary NCDS implementers, the acquisition community must establish policies reinforcing the goals of NCDS within their components. This section provides data-specific policy recommendations to establish acquisition deliverables compliant with NCDS direction:

- Establish NCDS as a requirement for program deliverables, including acquisition documentation.
- Establish UCore and C2 Core conformance as a C2 program requirement.
- Establish user-driven data consumption metrics for the C2 community as *the* ultimate measure of program success.
- Require programs to use existing, registered data and services, including vocabularies, to the extent possible.
- Require programs to engage in usefully constructed COIs (joint wherever possible, cross-CPM if feasible) to support C2 vocabulary and core development.

Implementation recommendations for each of these policies are provided in Section 4.0, Implementation Guidance Recommendations.

4. Implementation Guidance Recommendations

The Department is transitioning to net-centric operations. The requirements process is moving from programs to capabilities; the IT environment is moving from programs to enterprise, from producer-centric to user-centric, and from tightly integrated to net-centric/SOA. All of these changes impact organizational roles and responsibilities, governance constructs, and processes. As the community moves forward in implementing a C2 data sharing environment to meet the operational requirements, it will have an opportunity to engage the enterprise and help shape required new management constructs and processes. During the study, the IAT developed specific C2 data sharing implementation recommendations by organization, recommendations specific to implementing the C2 Core, and recommendations on key processes.

C2 Core was initially defined by JFCOM as a conceptual model composed of JC3IEDM sections related to essential entities and relationships, which are common and essential to all C2 activity. In this report, this initial work is referred to as the JFCOM-defined C2 Core. The IAT re-defined the C2 Core to: 1) encompass required run-time constructs, 2) reduce risk where artifacts, processes, and the C2 and enterprise IT environments are being created asynchronously, and 3) drive development of capabilities that are operationally responsive. This report re-defines C2 Core as consisting of: 1) a C2 Information Sharing Framework to support C2 IT development and operations; 2) a Joint C2 Conceptual Model and Joint C2 Vocabulary to provide context and the current C2 vocabulary, 3) C2-Specific Extensions from UCore to facilitate data sharing within the C2 community; and 4) C2 Core Service Specifications for C2-specific services. C2 Core is a decentralized environment with the necessary common facilities for sharing information required to command and control forces. The C2 Core builds upon the Department's enterprise IT environment. To the extent possible, C2 IT relies on Net-Centric Enterprise Services (NCES), augmenting NCES services to meet C2-specific requirements and, if required, to provide more general services not available through NCES. The components of the C2 Core are:

- **C2 Information Sharing Framework (C2ISF):** The infrastructure that enables data sharing necessary for C2. This infrastructure, which exploits DoD enterprise infrastructure, includes registries (services and metadata), content catalogs, access control arrangements, mediators, crawlers and tagging engines, development and test tool kits, and instrumentation to provide user feedback, metrics collection, and fact-checking capabilities.

- **C2-Specific Extensions from UCore:** C2 schema and vocabulary providing the ability to share data within the C2 community. C2-Specific Extensions

from UCore should be under configuration management of the C2 CPM in cooperation with the C2 community.

- **C2 Core Service Specifications:** These specifications define, specifically and functionally, the cooperating C2 mission services that actually perform functions required to support C2. Physical schema representation may or may not be specified.

- **Joint C2 Conceptual Model and Joint C2 Vocabulary:** A service that publishes descriptions of C2 entities and their interrelationships together with terms and definitions that express properties of those entities.

General implementation recommendations are captured below, with organizational and high-level C2 Core recommendations in the following sections. Additional notes on implementation can be found in Appendix D. The key process recommendations are in Section 5.0, Process Recommendations, and in Section 6.0, Enterprise IT Findings and Recommendations.

- Expect and plan for change. The ability to rapidly support new operational requirements is an advantage and is the benefit of implementing a loosely-coupled SOA where data and services are accessible to authorized users at any time and in any place.

- Advocate the use of UCore and C2 Core for C2 capabilities and use of UCore for non-C2 data sources that support C2.

- Establish a process for acquiring non-C2 data sources that support C2 operations.

- Direct the development and configuration management of a C2 Core as re-defined in this study.

- Emphasize collaboration among COIs and Component PEOs/PMs using portfolio management constructs to achieve C2 data sharing objectives.

- Direct that Component PEO/PM development teams subscribe to C2 Core services, employ artifacts when appropriate, and create new or updated C2-specific artifacts with COI support (this improves all programs' responsiveness to warfighter data requirements).

- Exploit the ISP required by current DoD directives as a preferred means for PSAs, CPMs, and other oversight entities to gauge C2 progress in implementing NCDS across the DoD enterprise.

- Establish an objective for the C2 CPM (ASD (NII)/DoD CIO and Commander JFCOM co-leads), selected COIs, and Component PEOs/PMs to collaboratively define utilization metrics for the developmental, pilot and operational C2 environments. Work with C2 development and operational centers to instrument the IT environment to collect service, data, and metadata usage metrics and other data sharing indicators.

- Establish an objective for the C2 CPM, the Services, and operational C2 organizations to streamline the identification and publication of data sharing requirements, prioritize and refine those requirements, and synchronize data exposure initiatives to support those requirements across the Department.
- Establish an objective for Component PEOs/PMs to include data, service and metadata utilization metrics in required test and evaluation strategy documentation including the Test and Evaluation Master Plan (TEMP).
- Direct the C2 CPM to use collected metrics and user feedback to assess utility, measure NCDS implementation progress, and recommend adjustments in C2 investments.
- Shape strategies to achieve the desired data sharing within a net-centric (vice mainframe/client-server/relational database) environment. Investment costs vs. ROI and affordability should be carefully considered.

The following recommendations are appropriate for use in specific implementation guidance and are covered in more detail in Section 5.0, Process Recommendations:

- Outline, flesh out and refine the data implementation plan for the C2 community noting dependencies on the enterprise IT environment and adjusting accordingly.
- Develop, maintain, and communicate a detailed description of C2 Core, its components, its mechanisms, its scope, and how it is used.
- Add infrastructure to support process, artifact publication, and management. A number of start-up capabilities are available but uncoordinated.
- Instrument development environments to assess *compliance* and the operational environment to track usage/utility and steer investment.
- Take specific steps to expose and allow broader exploitation of existing mediation artifacts and services, which comprise a key part of implementation.
- Address big CM challenges, including full lifecycles for services.
- Monitor and test to verify conformance to the vision not only during development, but post initial operating capability (IOC).
- Take affirmative action to make governance and process management, infrastructure and artifacts far more flexible (adaptive).
- Increase transparency through policy (seeing is believing) and adopt collaborative processes and tools for knowledge-based governance.
- Levy requirements and assign responsibilities and near-term deadlines for advancing IOC of the required supporting infrastructure.

4.1 C2 Data Sharing Implementation Guidance by Organization

4.1.1 ASD (NII)

- Review actual data metrics against forecast for compliance, progress, and operational utility (results).
- Use resources to support monitoring and enforcement of data policy within the C2 community.
- Scale delegated authority based on policy compliance and operational metrics (e.g., reputation management and participation).
- Ensure acquisition documentation supports NCDS, as recommended in the Acquisition Guidebook.

4.1.2 C2 CPM

- Establish and maintain operational focus. To meet C2 CPM responsibilities, the C2 CPM must be clear on operational priorities, their operational impact, and how these tie to proposed IT activities.
- Identify end user best value. The C2 CPM must be aware of acquisition and technical limits to identify and prioritize, on behalf of the C2 end user, data and service delivery that is highly valuable to that end user.
- Establish current IT and acquisition situational awareness for the C2 community. (See Appendix E for a possible approach to increasing situational awareness, speeding interactions between development and operations, and enhancing operational responsiveness[5].)
- Establish an open, participatory C2 Core management process. The C2 CPM and artifact publishers should jointly establish an open, participatory process to (1) populate and maintain C2 Core, (2) certify extensibility, and (3) lifecycle-manage C2-Specific Extensions from UCore 2.0.
- Communicate operational goals. The C2 CPM should relentlessly communicate the vision and goals for IT support to operators in both acquisition and operational terms. The C2 CPM should collect, analyze, and publish operational metrics and associated trends and let those numbers speak to the C2 constituency. This will allow the C2 CPM to stay above the fray when identifying poor suppliers. The C2 CPM should be the first and most vocal proponent of the current plan. If there are challenges, they should be

---

[5] "And how do we institutionalize procurement of such capabilities – and the ability to get them fielded quickly? Why did we have to go outside the normal bureaucratic process to develop counter-IED technologies…. Our conventional modernization programs seek a 99 percent solution in years – the wars we are in – require 75 percent solutions in months." Secretary of Defense Gates, Address to National Defense University, September 29, 2008.

resolved outside of public forums. The C2 CPM represents the C2 community to the DoD, as well as to the broader world. The C2 CPM must improve and uphold the C2 community reputation as a principal responsibility.

- Define and assign responsibility for C2 Core life cycle artifacts and processes (see Section 4.2, C2 Core Implementation Guidance).

4.1.3 Component PMs/PEOs

- Establish and apply procedures to ensure data and related services are visible, accessible, understandable, and trusted and included in acquisition documentation.
- Develop a comprehensive (development through end-of-life) CM approach and supporting processes that track all program deliverables throughout their lifecycle, including development and run-time artifacts and all acquisition documentation.
- Use the ISP to ensure acquisitions support the intent of the NCDS as described in the Acquisition Guidebook, Sections 7.4.2-3.
- Make sure that both the Test and Evaluation Strategy (TES) and Test and Evaluation Master Plan (TEMP) address data sharing, including required components (e.g., mediation services, registry entries).

4.2 C2 Core Implementation Guidance

The IAT developed candidate technical implementation recommendations as a function of current tools and the expressed needs of the C2 development community. This section represents a compilation of that information for use by the C2 CPM and the C2 community as they begin the process of defining and maintaining the C2 Core. The IAT recommends directing the C2 CPM to define and assign responsibility for C2 Core life cycle artifacts and processes.

C2 Core Definition and Compliance: To define a meaningful evolution of the C2 Core and ensure its broadest possible application and use, Component PMs and PEOs should:

- Nominate candidate data components and services for inclusion in C2 Core, to include vocabularies, taxonomies, service specifications and performance or access limitations, content catalogs, service registries and entries (including data and metadata), mediators, crawlers, tagging engines, development and test toolkits, and instrumentation to provide user feedback, metrics collection and fact-checking capabilities.
- Actively participate in the on-going C2 Core definition and vetting process.
- Source, as assigned, C2 core data and data services over their lifecycle.
- Articulate and maintain current C2 core data and services source lifecycle commitments via a Lifecycle Support Agreement and Lifecycle Timeline.

- Automate run-time reporting of data source and service availability, consumption, and select C2 user-experienced performance.
- Collate, publish, and analyze data source and service availability, consumption, and select C2 user-experienced performance throughout the source lifecycle (development, pilot, operations).
- Collect, publish, and analyze data source and service problem reports throughout the source lifecycle (development, pilot, operations).
- Automate run-time reporting of data and service consumption in support of an "always current" Interoperability Matrix.
- Define, in concert with the C2 CPM, objective UCore extensibility definitions and test harnesses for certification of extensibility.
- Define, in concert with the C2 CPM, objective conformance metrics and test harnesses for C2 Core.

C2ISF. This framework must use existing enterprise services along with existing, foundational C2 operational IT elements. The following list, while not inclusive, provides a minimum set of essential elements that should be considered to operationalize this capability:

- NCES-provided enterprise services. (Of particular concern and foundational to all of these efforts is the definition and federation of individual identity and a permissive approach to access controls)
- UCore Version 2.0
- Shared Situational Awareness Track Framework (SSATF) as a set of candidate C2 components for run-time data and data service offerings
- Data Mediation Framework for C2 (i.e., I3 Data Services and toolkits)
- C2 Visualization Framework (i.e., I3 Visualization Framework and toolkits)
- C2-specific MDR community
- JFCOM-defined C2 Core vocabulary (to be extensions of UCore)
- C2-specific DDMS community data
- Commercial metrics collection and analysis capability (e.g., omniture)
- Web Service Definition Language (WSDL) checkers.

Joint C2 Conceptual Model and Joint C2 Vocabulary Service: This service represents a federation of structured and unstructured data models and the navigation and organization service that makes them easily accessible. It establishes a concept of a joint and combined mission space, and of common C2 entities, including vocabularies, and their inter-relationships. For those data destined to be represented in a relational model, the IAT recommends:

- Maintain a Web Ontology Language (OWL) Description Logics (DL) version.

- Publish model vocabularies and valid values as a Web service with user-friendly navigation and download capabilities.
- Maintain and publish a mapping of logical models to physical schemas as well as mappings to support mediation where warranted.
- Coordinate among the various messaging standards activities to identify candidate common vocabularies, valid values and conceptual content.

C2-Specific Extensions from UCore: C2 schemas beyond the scope of UCore, but essential to the community, will be integral to C2 Core. A partial list of existing source schema that could be used as the C2 community populates the C2 Core includes:

- Standard message formats (e.g., USMTF, OTH-G, VMF, TADILs (tactical digital information link))
- Standard military symbology (e.g., MIL-STD-2525)
- XML schemas already published in the MDR
- Mediation schemas scoped based on mission threads, cross-COI or cross-format types.

Common Data Services for C2, including C2 Core Service Specifications. The IAT recognizes that common data services for C2 will exist and emerge that, for various reasons, are not incorporated into the C2 Core. In fact, if the Department is successful with NCDS, this will become the default, rather than the exception. Therefore, the IAT recommends:

- C2 Core concepts and vocabulary should be represented using any of the physical schema types supported, depending on the service or application context. These could include Relational Database Management System (RDBMS)/Structured Query Language (SQL), Hyper Text Markup Language (HTML), and Really Simple Syndication (RSS).
- C2 Core concepts should be reused and represented in common C2 Core service offerings. For example, C2 Core vocabulary and tags within an operational context should be used *as is* in C2 Core service specifications. C2 Core services should be viewed as the mechanism for exposing, manipulating, and producing C2 Core-compliant data and metadata.

5. Process Recommendations

C2 implementation and operation will be supported by processes that touch almost every organization, but for the most part, these processes are not owned by the C2 community. The IAT noted the importance of these processes to the development and operation of the C2 data sharing environment and developed the following recommendations based on their observations and experience. Implementing the recommendations in Sections 5.0 and 6.0 will require dialog with and among many stakeholders and process owners.

5.1 Operational Needs and IT Implications Assessment

For successful NCDS implementation, the following steps are recommended:

- Capture and understand current operational needs and context as it is and not as we wish it to be. (In this sense, concepts of operation (CONOPS) and TTPs that exist on paper suffer from the same fate as approved IT standards. They are a good basis for understanding commonality in current capabilities, but cannot reflect what is emerging at the edge. Only real-time assessments can capture and help make sense of current edge phenomena.)
- Define the IT implications for data sharing (data and data services), including *good enough* parameters.
- Identify possible data sources, to provide a sense of the overall portfolio and available offerings, including emerging offerings.
- Articulate lifecycle costs in both operational and acquisition terms.
- Assess and effectively communicate competing priorities based on user needs, operational impact (breadth and depth), cost and risk.
- Communicate the operational value proposition, including projected consumption metrics over time. This can be enhanced and offloaded by enlisting an articulate functional proponent willing to champion and pilot the activity.
- Monitor product release and consumption uptake, including piloting. This must include monitoring supporting release functions, such as updating compatibility/interoperability matrices, training, and product announcements (operator communications).

5.2 Measuring Program Success via User-Driven Consumption Metrics

Too often, the impact of IT upgrades or the introduction of new capabilities cannot be articulated. In addition, each part of the IT provisioning chain has an insufficient stake or visibility to the operational impact to motivate common go/no-go decision criteria. To motivate common vision and focus, Component PMs and PEOs should:

- Project user consumption metrics (over time) for all data sources or service investments exceeding pre-established programmatic thresholds.
- Provide projected user consumption metrics and operational effectiveness impacts as key components in any investment decisions exceeding pre-established programmatic thresholds.
- Track actual user consumption metrics versus projected consumption metrics and assign or adjust individual reputation values for an entire IT capability provisioning team (formal requirers, portfolio and program managers, developers, testers, IT operators).

5.3 Leveraging Existing, Registered Data and Services

Component PEOs and PMs should require that constituent programs consume, preferentially, C2 Core data and data services and register their subscriptions, service information, and publication/consumption artifacts at the earliest possible moment. Developmental artifacts should be registered before IOC to make insipient data sharing relationships visible at the earliest possible moment.

5.4 COI Engagement

The only community mechanism for collaboratively identifying and specifying C2 core data and services is the COI. COIs are the only cross-organizational forums available to address technical issues associated with data sharing implementation among capabilities fielded by multiple Component PEOs/PMs. The COI Registry is the only mechanism that provides broad visibility into who is doing what in the data sharing arena. Therefore, Component PEOs and PMs who source or consume C2 core data or services should:

- Actively participate in all consuming COIs (those that have a dependency on the Component PM/PEO source data) and actively monitor all contributing COIs (those whose data the PM/PEO consumes)
- For source data that is not part of current C2 Core data and services but whose consumption data indicates use that is broader than the sourcing Component PM or PEO, identify the responsible COI, provide consumption metrics, and actively participate in accepting responsibility for or transitioning the data or service to the C2 Core.

5.5 Types and Examples of Metrics

Two types of metrics are generally indicative of data or service offering success: *development metrics* and *run-time metrics*.

Development metrics are collected during development, integration and test phases of an effort. Best commercial practices in the IT industry include:

- *Problem report open and close rates.* A rule of thumb is that no service should be piloted or operated until the problem discovery rate lags the problem close rate. That is, the number of new problems reported on a daily basis is less than the problem closure rate. Until this is the case, the service is too immature for operational use.
- *Test coverage.* Component PMs and PEOs should understand the test coverage for test harnesses available for a service or capability. The higher the percentage of test coverage, the less likely there will be a catastrophic failure in fielding. Any proposed test that does not significantly increase the overall test coverage should be questioned. In addition, problem reports from operations should be used to extend development phase test coverage. Although it is often not possible to replicate fully the operating environment, each operational problem report should be evaluated for root-cause analysis with a possible proposal for how to update the capability test harness to address the failure.
- *Configuration control.* Given the plethora of workstation configurations in the DoD inventory that will potentially be consumers or subscribers to data and services provided by the C2 community, the likelihood of client-induced failures increases. In coordination with component CIOs, the Component PMs and PEOs should define and acquire workstation configurations consistent with common user base workstation configurations, reducing the potential for failures based on workstation-related infrastructure components (e.g.,browsers, operating systems, firmware, drivers).
- *Performance benchmarking*. To achieve a true understanding of the user experience, gangs of workstations that are identically configured should be employed to performance test user-facing capability between releases. In this way, the Component PM and PEO will have a true indication of the impacts of ongoing changes to the user experience in a clean environment. If the field perception is that a new service release is slow, but the PM knows that internal tests showed the same or faster performance, the PM may begin diagnostics confident that something in the operational environment is the problem. The PM may still need to fix the supplied service, but significant trouble-shooting time will be avoided. Similarly, if the PM discovers a decrease in performance since the last release, the PM may address specific performance attributes in the current or subsequent release.

Run-time metrics are collected during pilot and operations phases of an effort. IT industry best commercial practices include:

- *User-perceived service availability.* Through appropriate architectural use of commercial virtualization technology, the uptime of service offerings can trivially approach an availability of five 9s[6], even though the component parts have lower individual availability. It is important to measure this using the same or similar communications paths as the user; accessing an offered service on an internal path does not replicate the end-user experience.
- *User consumption.* This measures actual invocation of data or service in an end-user context. The simplest of these tools involve Web-page beacons that collect page invocation counts and provide them to an assigned collection agent using short messages. User invocation context may also be collected if the workstation collects cookies. Much more sophisticated mechanisms, including loggers and business analytics frameworks are available. The goal is to meter user consumption with a purpose of understanding what is of most value to an end user.
- *User-perceived performance.* This measures the end-user experience and is typically a set of elapsed-time measurements that reflect a user's wait time for service response or data display. For example, the time from when a user requests a Web page to the time it begins to appear on the screen is a common performance metric.
- *Performance factors affecting the user.* These are non-subjective measures that identify real and perceived delays in response time (response time delays for receipt of data from a data source after a request has been issued, display time delays from the time of receipt of the data from the data source to the completion of the page display, etc.) These are quantitative measures amenable to being gathered and recorded automatically without human involvement. With such metrics one is able to better ascertain the base causes of the subjective user perceived performance failures.

The goals for metrics collection and the indicators likely to best illuminate those goals should be articulated. Component PMs and PEOs should also consider possible unintended consequences of specific metrics. For example, the broad use of Web-page counts has resulted in fewer scrollable pages and more clicks to the next page, as content providers strive to increase their page counts, industry ratings (a la Nielsen), and associated advertising revenue.

5.6 Reputation: Assignment, Monitoring and Reporting

A reputation range is defined with every participant starting at the midpoint. Positive or negative contribution to a fielded capability increases or decreases the reputation, respectively, and positive reputation is reinforced through rewards, recognition, bonuses, and communications. More reputation is gained when a team delivers on time, within budget and achieves their projected launch rates (user consumption projections). Less

---

[6] When an IT system operates 99.999% of the time, it has 5.4 minutes of downtime in a year.

reputation is gained when a team delivers on time, within budget, but misses launch rates. Reputation is lost if a team delivers late, over budget, and misses launch rates.

Both individual and organizational reputations are maintained and adjusted, as capability is fielded (or schedules missed), resulting in aggregates for the organization, as well as individual contributors. Every discipline (requirers, portfolio managers, acquisition oversight, Component PMs/PEOs, test community, IT operators) is represented, so all participants are motivated to engage early in the capability or service definition so as to enhance their reputation through achieving a mission-focused goal.

Obviously, discipline is required to instantiate and to maintain this process. Cross-vertical team members must participate in early capability and service production efforts, or those individuals later in the production cycle (test and operations) will have reputation scores that are not reflective of their contributions.

Go/no-go criteria become crisper as individuals and organizations focus on how to get to the field with secure, reliable, useful capability.

5.7 Complete Lifecycle Configuration Management

Since certain classes of service offerings cannot be tested in a stand-alone environment (e.g., millions of notification messages) the fielding readiness assessment must be broken into composite parts. Root-cause analysis is performed to determine where the software or infrastructure is likely to break. Specific failure cases are tested (e.g., 35,000 notifications/second) in special purpose test harnesses to achieve some level of assurance that the specific failure mode has been addressed. The capability is then rolled out to a subset of the operational community and closely monitored by operations. If queues do not build and the service continues to work under load, the user population is grown and the cycle repeats itself until the service is fully deployed. If, at any point, operations detects a critical failure or cascading effects likely to result in a critical failure, a complete image capture of the run-time environment is made for diagnosis and the new capability is pulled from operations.

The implications for configuration management are obvious. A capability in development must be presented, as is, to the test environment, where it can be exercised within the limitations of that environment. The same capability must then be presented to a limited subset of the operational environment and assessed for broader application. Finally, there must be an ability to quickly remove a service or capability that causes a catastrophic failure (or simply to retire that capability). In the case of failure, IT operations must provide adequate feedback to develop and test to (1) correct the problem and (2) update the test harness for future detection and correction. In the case of retirement, IT operations must provide adequate feedback to development and test so that resources allocated to maintenance of the capability may be reprogrammed.

A number of classical CM products recognize and support these lifecycle needs. Portfolio managers, and Component PMs and PEOs should reflect this view in their CM plans and begin the necessary planning and dialogue now with constituent stakeholders.

5.8 Net-Centric Testing

Although DoD does perform a great deal of service-level conformance testing, it has little experience with data compliance testing. The experience that does exist is a result of verifying compliance with or among logical data models and is usually marked by manual processes. With the emphasis on run-time, this clearly will not support NCDS goals.

Specificity of compliance requirements must be sufficient to provide development and test toolkits that assure compliance goals, which may include interoperability, discoverability, and consumability. Warrants of compliance should be backed by raw toolkit outputs. Ideally, warrants should be accepted cross-Service and cross-Agency without repeat verification.

Virtualization of wide-area connectivity is already accepted in the DoD development and test community, sometimes to the detriment of the bandwidth-disadvantaged user. Because of the strides in virtualizing storage and computing, DoD data and service providers are using this capability to reduce costs and increase end-user-perceived reliability and availability. The development and test community must proactively work to characterize and describe use of virtualized storage and computing such that separate verification of the virtualized run-time or storage is accepted without requiring retest of the underlying virtualized components.

Virtualization is also provided at higher orders in the stack (e.g., Web and mail services) through the use of load balancers. In effect, gangs of blade servers, identically configured to serve up content (Web pages and mail) are tasked dynamically by the load balancers based on server load and projected distribution requirements. In certain cases, blade servers may be dynamically switched into the operating environment to handle peak loads. Again, the development and test community must proactively work to characterize and describe the use of load balancers and ganged identical application servers so that the data and functional service tester does not require retest of the underlying components.

Finally, NCDS and other Departmental policies, dictate a level of data and functional interdependency heretofore unknown in the Department. Although no Component PM or PEO has ever controlled all aspects of their environment, the acquisition community has largely closed their eyes to this reality and required end-to-end testing based on POR boundaries. NCDS drives this level to the service (subroutine) and data element level. Capability-based testing demands refinement of boundary conditions and definitions and will, no doubt, constitute first steps in grappling with how to sufficiently test in a truly net-centric run-time environment. The development and test community must pilot new thinking and new methodologies to characterize boundary conditions to understand how and when to invoke scaled levels of testing, as well as the limits of classical testing approaches.

The IAT strongly recommends that the C2 community work with OT&E on these issues. Test community leadership should take an aggressive and pro-active role in redefining

their testing approaches and re-educating their employees and stakeholders to these new approaches. This should include clear communication of what is expected in both a TES and a TEMP with respect to data. Since the community will tend to return to current practices, test community leadership should establish clear metrics, tied to operational effects, which incentivize the cultural changes necessary to move to net-centric test practices. Among other things, test facilities should leverage live operational environments around the globe, actually subscribing, wherever possible, to published data sources to use as test artifacts.

5.9 Service and Platform Definition and Governance

Specifics of the technology offerings should be defined by a technically competent, responsible individual best attuned to the end user functional needs and the realities of the underlying technology stack. Community governance should be aware of the decisions and informed, to the extent they are interested, in areas of disagreement and why certain technological courses of action have been selected.

Community governance of platform and services should be focused on the *what* and not the *how*. Community representatives should participate in reputation assignment and management and should be chiefly interested in platform consumption metrics and operational impacts (like a board of directors).

Service Level Agreements (SLAs) should be developed and registered in a service registry. The registry should contain metadata to support identification, comparison, selection, access, and interpretation of service offerings. The metadata about a service constitutes the promise or agreement of the service provider to its users. Performance measures such as response time and availability should also be registered. Entries describing version timelines, backward compatibility, etc., should also be included in the registry metadata and be part of the SLA. The registry should contain identification and specification of data published via the service, for both quality and structure of content. In effect these entries in the service registry are contracts between the producer and consumers. The C2 Core should support and utilize SLAs.

6. Enterprise IT Findings and Recommendations

As noted earlier, the move to an enterprise information environment is a change. The C2 information environment will operate in and across this DoD-wide environment, and should take advantage of enterprise data services. At this time, not all of the planned enterprise services and governance constructs for managing these services have been implemented. The C2 community will need to assess status and plans and adjust accordingly. This section provides findings and recommendations on topics that are the result of the move to an enterprise, net-centric, SOA environment and/or are not specifically under the control of the C2 community.

6.1 Metadata Environment (MDE)

Insufficient attention has been given to this essential infrastructure capability that is key to enabling the C2 community (and the rest of the enterprise) to execute the Net-Centric Data Strategy.

Finding: Insufficient effort has been devoted to building, identifying, operating, and federating powerful suites of cooperative metadata engines on which the NCDS depends.

Collectively, the various metadata handling capabilities required to support DoD's operational and developmental IT activities are termed the MetaData Environment (MDE). These are infrastructure services, tools and processes associated with exposing and managing the full life cycle of metadata. Their mission is to enable the visibility, accessibility, and understandability of capabilities and content. The trustworthiness, security, and interoperability of data the Department uses are also dependent on well-organized metadata efforts.

Using C2 as an example, the C2ISF, Core C2 services, and C2-related data sources (authoritative and others) constitute community-specific components of a close-knit MDE. Many communities are working with these same concepts today, emphasizing support for run-time capabilities. The build-time MDE for C2 includes conceptual models and vocabularies, Core C2 Service specifications, schemas and other data sharing package components, associated governance and lifecycle management repositories, toolsets, and services (e.g., CM, release management and interoperability matrices).

These C2 (or any community's) metadata capabilities are not freestanding. To deal with the requirement for a DoD-wide reach and to deal with the other government and NGO/commercial information sources on which Department operations depend, numerous non-DoD metadata services must be exploited. Metadata support must, therefore, involve an ongoing, adjustable collaboration with the COCOMs, Services,

Agencies, key non-DoD activities (e.g., the Intelligence Community and Department of Homeland Security), allied and coalition partners, NGOs, and commercial entities.

Recommendations:

- Launch a much broader, concerted approach to address metadata needs. Distribute the action as follows: (1) General purpose enterprise metadata capabilities, (2) Community-specific metadata capabilities, and (3) Non-DoD metadata capabilities. Work out how to federate these capabilities both for short term, on-the-fly requirements and long-term cooperating arrangements.

- Flesh out patterns for (1) a build-time infrastructure for rapidly bringing required capabilities to IOC and (2) deploying a run-time infrastructure that enables the data sharing necessary in any C2 operational context globally. The nominal MDE definition and design effort would exploit DoD enterprise infrastructure, emergent community infrastructures, and non-DoD metadata services, potentially including registries (e.g., service and structural metadata), content catalogs, access control arrangements, mediators, crawlers and tagging engines, development and test tool kits, and instrumentation to provide user feedback, metrics collection, and fact-checking capabilities.

- Establish a decentralized run-time set of metadata-centric infrastructure capabilities to provide an operational environment for sharing data.

- Apply the same principles to create a net-centric development environment (to enable discovery and access) and connect the operational and developmental environments.

6.2 Portfolio Management

The Department appears to have conflicting portfolio management policies.

Finding:

DoD has two portfolio management directives (8115.01, "Information Technology Portfolio Management," dated October 10, 2005, and 7045.20, "Capability Portfolio Management," dated September 25, 2008) and one instruction (8115.02, "Information Technology Portfolio Management Implementation," dated October, 30, 2006). DoD Directive 8115.01 is focused on IT portfolio management, and with the companion instruction outlines processes for portfolio management at the domain and mission area levels, and establishes procedures for working across domains and mission areas. DoD Directive 7045.20, which was signed during the course of this study, is focused on capability-based portfolios and is based on experiences gained in piloting four capability portfolios, one of which was C2.

The C2 Capability Portfolio is largely IT, but appears to be continuing the pilot work and heading towards compliance with DoDD 7045.20, rather than DoDD 8115.01. The

Capability Portfolio Manager role under DoDD 7045.20 is an advisory, rather than directive, role.

Recommendations:

- ASD (NII) should advocate for elimination of conflicting portfolio policies, especially with respect to C2 IT.
- Under ASD (NII) guidance, the C2 community should develop governance constructs consistent with the appropriate portfolio management directive.
- If DoDD 7045.20 is the basis for C2 portfolio management, NII and JFCOM should advocate for the addition of appropriate management constructs to support cross-portfolio data dialog and resolution of issues related to COI management, lifecycle support agreements for data sources, adjudication of issues, etc. Some of these constructs exist (e.g., adjudication) in DoDD 8115.01.

6.3 COI

The relationship between COIs and the organization need to be defined and DoD Directive 7045.20 did not address this requirement.

Finding:

COIs, as described in the NCDS, have been established in the Department for several years. The slow progress in specific areas may be attributable in part to:

- Lack of focused sponsorship: This may be due to the immaturity of C2 service definitions and implementation, as any service-development and maintenance effort needs a strong producer-consumer relationship to flourish. Well-known relationships among existing PoRs and user groups have been used, but inconsistently.

- Funding issues: COIs are intended to support multiple programs and to be used jointly wherever feasible. However, funding is generally program specific.

- Inadequate or immature enterprise infrastructure: The enterprise infrastructure to support enterprise-wide use of COI results is not yet in place.

Recommendations:

To make more effective use of the COIs, the IAT recommends that the C2 CPM, as formalized in DoDD 7045.20, take a strong role in assessing progress and advocating for funding for COIs that are supporting efforts that are essential to the C2 community. As the advocate for such COIs, the C2 CPM should:

- Assess the visibility, accessibility, and understandability of data across the C2 portfolio and by users of portfolio capabilities.

- Advocate for funding for COIs where there are gaps.

- Although the new Directive does not define management roles for the CPMs, the IAT believes that there are two management functions that should, at a minimum, be reviewed by the CPM. These are to: 1) review and advocate for cross-CPM COI activities (for example between Battlespace Awareness and C2), and 2) ensure proper lifecycle management of COI artifacts after the COI has completed its work (for example, making sure that the entries in the MDE are maintained to support users over time).

- Review data artifacts, architectures, and plans provided by PoRs within the C2 portfolio to assess progress in meeting C2 community needs. Specifically, the C2 CPM should review the data products in the Acquisition Guidebook as being required prior to both Acquisition Milestones (MS) A and B. This includes: 1) a Net-Centric Data Sharing Plan that outlines how a program's data and processes will be made visible, accessible, and understandable as called for prior to MS A; and 2) a data plan that prioritizes data assets and identifies required COIs, as called for prior to MS B.

6.4 Existing Message Standards

Data standards and formats, used by the C2 community, are managed by disjointed processes.

Finding: Currently there is a plethora of data standards and message format-related bodies in the C2 area. Examples include, but are by no means limited to, USMTF, VMF, Link 16 TADILs (tactical digital information links), GBS (Global Broadcast Service), OTH-Gold, etc. Each of these involves CM activity and often covers similar kinds of data represented in different formats. This creates interoperability problems. Although overarching messaging standardization work is ongoing, it exists in parallel to every competing messaging standard subset and its associated governance structures and processes. There appears to be no concerted effort to reconcile (and possibly collapse) competing or duplicative messaging activities by clearly articulating target transition points.

Recommendation: Work with the Joint Chiefs of Staff, COCOMs, Services, and Agencies to coordinate, consolidate and converge the data and message standards currently active in DoD.

6.5 Governance Processes for C2 Data Sharing Among Partners

Multi-national participation is essential, because the issues are broader than DoD and broader than the US.

Finding:

One of the significant advantages of the MIP work on JC3IEDM is the existence of a working standards body that includes many of our partners and is focused on the C2 space. MIP provides a working vocabulary and conceptual model for C2, both of which have been negotiated among its constituency. Still, based on US experience to date, it appears unlikely MIP will drive all data standards for C2, at least not (NOT SURE THIS IS RIGHT?) in the near term. In part, this is the dilemma of all standards bodies--operational changes occur at a faster pace than traditional standards bodies can support. In part, it is the issue of transitioning a very large legacy environment.

The IAT performed an analysis that compared current *uber* messaging signatories and implementers to coalition partners in Afghanistan and Iraq. Unfortunately, only 30 percent of the countries participating in current operations in those two areas of operation (AORs) are also involved in this overarching messaging consolidation activity. Further, DoD messaging activities, in general, do not encourage nor allow for participation by NGOs, which figure heavily in all stabilization operations.

The best way to get NGOs involved is through aggressive participation in and use of standards bodies. As an example, the National Geospatial Agency (NGA) used the Open Geospatial Consortium® (OGC) to develop and field the Geographic Information System (GIS) standards. First, this approach provides a forum where Government representatives and NGOs can work together without violating the sensitivities of either side. Second, the results are driven back into commercial (non-defense unique) software that facilitates interoperability. Much of the JC3IEDM can be addressed in these forums because of its inherent abstraction.

Similarly, there is a major market for first-responder C2 tools and services. NGOs in the 2004 Asian Tsunami relief effort used collaboration software, as did first-responders and NGOs in the Southern California fires. Also, NGOs used social networking sites during Hurricane Katrina relief operations.

Recommendations:

- Establish strong, agile, well-defined US CM processes that recognize the existence of, necessity for, and relationships with other standards bodies and CM processes

- Recognize that, in most situations, NGO capabilities are generally out of military control. Where there is a mismatch of interface standards, they must be treated as *black boxes* that can only be accessed or receive inputs via their published interface specifications. This is one of many cases for encouraging development of more powerful, agile mediation capabilities (see discussion below).

6.6 Run-Time

Very little focus on the run-time environment; eyes are on acquisition and development.

Finding:

DoD data activity is disconnected from data implementation activities. These activities must be refocused to further NCDS goals.

Recommendation:

Focus data and service activities on the operational information environment DoD-wide. Successful implementation of the NCDS must encompass the manifestation of data and associated data services in the run-time environment. This recommendation is clearly not unique to the C2 portfolio. To effectively operationalize the purpose and intent of NCDS, we must define and measure its impact on operational effectiveness. The focus must move from development to the operating environment; from a computer science perspective, this dictates an emphasis on the actual run-time environment. This activity must encompass pilot and test environments, but it must emphasize the operational run-time, which starts with identifying and prioritizing operational processes. Capabilities must be architected to reflect operational needs, to identify information IT infrastructure dependencies, and to support prioritization of scarce resources such as world-class troubleshooters and administrators.

Current DoD IT operations suffer from several significant challenges: (1) IT operators have little understanding of operational mission priorities until something breaks. (2) IT operators have little understanding of the impact on mission operations as a result of IT dependencies. (3) IT operations are generally decoupled from IT acquisition, so IT developers are free to make misguided design decisions that can result in non-field-sustainable capabilities. Focusing every part of the IT provisioning chain on the operational mission effects and end-user adoption rates of a capability will do much to address these challenges.

6.7 Mediation

Insufficient recognition of the requirement to provide mediation services.

Finding:

Many in the Department want to dispense with data mediation, although it is a critical tool in data sharing. Indeed, providing for powerful, agile mediation is a key feature of any successful information strategy. Mediation is frequently the fastest way to integrate a new information source, and it is required to deal with the asynchronous evolution of DoD's IT capabilities.

Recommendations:

- The C2 CPM should identify, highlight, and investigate means of rapidly providing mediation capabilities for key interface problems and where significant customer bases request different data sharing standards. (Mediation is routinely provided by PoRs in pursuit of required data feeds.)
- The C2 CPM should explore the option of a powerful, central C2 mediation service, which exploits all registered C2 metadata, mappings, etc., to bring up clusters of C2 interoperability on the fly.

7. Conclusion

There is (or should be) a clear distinction between a globally distributed, asynchronous, responsive intervention vision versus data sharing via a centrally directed *sameness* that the Department implements in blocks. Fundamentally, the latter is unachievable due to scale, complexity, and dynamics. Realizing powerful data sharing capabilities among DoD users and their partners, which is the objective, will only happen through an ongoing, user-prioritized series of enhancements that happen rapidly (just in time) at the edge as needs and opportunities arise and through a mature understanding of lessons learned and thoughtful interactions at the working level.

To enable the vision, we can make data engineering at the edge far more robust and responsive by, among other things, making a plethora of helpful artifacts and processes available online through services. This safely and proactively closes the gap between operations and acquisition.

Good work has been done in laying the foundation of understanding necessary to accomplish the vision. The IAT recommendations represent only the first step in a long-term and challenging change mandate, which touches every component and process in the IT provisioning chain. By addressing the IAT-identified challenges in a transparent, collaborative, operationally-focused manner, the C2 community will continue to set the standard of excellence for C2 around the world.

The IAT's strongest recommendation is for the C2 community to immediately develop and implement an operationally focused plan to incrementally deliver these capabilities to our forces.

Appendix A.
Glossary

Access: To interact with a system entity to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's resources.

Access Control: Protection of information resources against unauthorized access; a process by which the use of information resources is regulated by a security policy and is permitted only by authorized entities according to that policy.

Agility: The ability of an organization and its supporting systems to respond quickly to demands or opportunities.

Artifact: Tangible byproducts produced during the IT process. As used in this report, an artifact refers to objects generated to communicate, explain and otherwise bring clarity to shared understanding of data and how it is exposed during the IT life-cycle (concept development through implementation through operations) for human or machine use.

Attribute: a distinct characteristic inherent in or ascribed to an entity; an entity's attributes are said to describe it

Authentication: to confirm a system's asserted principal identity with a specified or understood level of confidence.

Authoritative: recognized by appropriate governing authorities to be valid, trusted or distinguished as preferred (e.g., the United States Postal Service is the authoritative source for U.S. mailing ZIP codes).

Authoritative Data Sources (ADS): Data products, including web sites, databases and broadcasts, which have been identified, described, and designated by DoD authorities as highly trustworthy for use in military operations support. Various CC/S/A organizations, the IC, other U.S. Government, allied/coalition organizations and NGOs etc. operate ADS.

Business Function: something an enterprise does, or needs to do, in order to achieve its objectives.

Business Mission Area (BMA): The BMA ensures that the right capabilities, resources, and materiel are reliably delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. In order to cost-effectively meet these requirements, the DoD current business and financial management infrastructure - processes, systems, and data standards - are being transformed to ensure better support to

the warfighter and improve accountability to the taxpayer. The Deputy Secretary of Defense leads integration of business transformation for the DoD business enterprise.

Business Process: The complete chain of actions and responses that are undertaken by some entity to provide a product and/or service for users. A business process entails the execution of a sequence of one or more process steps. It has a clearly defined deliverable or outcome. A business process is defined by the business event that triggers the process, the inputs and outputs, all the operational steps required to produce the output, the sequential relationship between the process steps, the business decisions that are part of the event response, and the flow of material and/or information between process steps.

C2 Core: Initially defined by JFCOM as a conceptual model composed of JC3IEDM sections related to essential entities and relationships, which are common and essential to all C2 activity. In this report, this initial work is referred to as the JFCOM-defined C2 Core.

This report redefines C2 Core as a decentralized run-time set of infrastructure capabilities which provide necessary common facilities for sharing information required to command and control forces. These capabilities rely on separation of data from applications in a Service Oriented Architecture for data access and discovery. Tags facilitate understanding of the data and rapid repurposing of data and services. Extensive use is made of metadata to describe the location, structure and content of data and services available to edge users. Knowledge of the meaning of the data accessible by edge users is available to authorized parties in forms suitable for machine processing. An environment is required to acquire, manage and publish this metadata. The C2 Core builds upon the Department's infrastructure to support C2 activities. To the extent possible, C2 IT relies on NCES augmenting NCES services to meet C2-specific requirements and, if required, to provide more general services not available through NCES. C2 Core consists: the C2 Information Sharing Framework, C2-Specific Extensions from the UCore, Joint C2 Conceptual Model and Joint C2 Vocabulary, and C2 Core Service Specifications (definitions for each are included in this Appendix)

C2 Core Service Specifications: These specifications define, specifically and functionally, the cooperating C2 mission services that actually perform functions required to support command and control of operations. Physical schema representation may or may not be specified

C2 Information Sharing Framework (C2ISF): The infrastructure that enables data sharing necessary for command and control of operations. This infrastructure, which exploits DoD enterprise infrastructure, includes registries (service, metadata), content catalogs, access control arrangements, mediators, crawlers and tagging engines, development and test tool kits, and instrumentation to provide user feedback, metrics collection, and fact checking capabilities.

C2-Specific Extensions from UCore: C2 schema and vocabulary providing the ability to share data within the C2 community. C2-Specific Extensions from UCore should be under configuration management of the C2 CPM in cooperation with the C2 community.

Community of Interest (COI): In the context of this report, a COI is any collaborative group of GIG users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange. The COI concept is very broad, and covers an enormous number of potential groups of every kind and size. Any element of a DoD Component, for example, domain, organization, task force, project team or group who must exchange information may be considered a COI. For example, every task-oriented workgroup (e.g., the bomb damage assessment cell at the Air Operations Center) can be a COI. Any collection of people with a declared interest (e.g., in biological warfare) can also be a COI. In DoD's Net-Centric Data Strategy, the main purpose of the COI concept is provide a publishable identity that makes cross-organizational groups visible and enables tracking of their mission, activities and composition. A COI Registry is operated on NIPR and SIPRNet so that users can discovery what COIs are active, what they are doing, and who is participating in them.

Conceptual Model: A map of concepts and their relationships. These models describe the semantics of an organization and represent a series of assertions about its nature. Specifically, they describe the things of significance to an organization (entity classes), about which it is inclined to collect information, and characteristics of (attributes) and associations between pairs of those things of significance (relationships).

Core Services: Those DoD enterprise and C2 services that are common to one or more multiple COIs of interest to C2 and/or multiple C2 programs. Identification and definition of core services should (1) support finding and accessing relevant information; (2) expose produced information for discovery and consumption of others, including unanticipated users; (3) support effective and confident collaboration; (4) seamlessly stage data throughout the C2 community, including DIL users; and (5) improve the user experience with respect to data performance and reliability.

Data Component/Metadata Component Discovery: The MDR allows users to browse for metadata artifacts by namespace, by category, and by using an advanced search capability that allows for searches based on the combination of the artifact names, associated service(s), and other attributes.

Discovery

> **Enterprise Web Services Discovery:** DoD enterprise web services provide access to DoD-wide software capabilities over DoD networks and the Internet using standard protocols. The NCES Service Discovery capability allows users to browse for services by service provider, by category, and by using an advanced search capability that allows for searches based on the combination of the service name, service provider, and other attributes. Examples of DoD enterprise web services include identity and security management.
>
> **C2 Web Services Discovery:** C2 web services, likewise, provide access to C2-specific software capabilities over DoD networks using standard protocols. The C2 Portfolio Services Discovery allows users to browse for services by service

provider, by category, and by using an advanced search capability that allows for searches based on the combination of the service name, service provider, and other attributes. Examples of C2-specific software capabilities include association and correlation.

DISR: The DoD IT Standards Registry (DISR) describes authoritative sources for Information Technology Standards in use by the Department and profiles of IT systems that employ them.

Distributed (or Decentralized) CM: In a massively distributed environment like the GIG, developers are facing conditions that involve the coordinated use of multiple engineers often from different organizations working at multiple sites on a system or a set of interdependent software capabilities (i.e., a federation) or significant components thereof. In the extreme case, multiple DoD and non-DoD organizations in multiple countries form coalitions that may involve producing, maintaining and using a specific artifact for data sharing. In such a setting, configuration management becomes a serious challenge. At the highest layer, there is the issue of integrating the asynchronous efforts of engineers who may be adhering to different CM procedures and practices. Distributed CM seeks to unify these. In the middle layers, issues of providing distributed data management are encountered. Distributed CM assigns managers to collaborative control and publish attributes of data component versions.

DoD and non-DoD Sources: Information capabilities running on both commercial and government networks funded and operated by the Department of Defense as opposed to those put up by other government or NGO activities.

DoD-wide C2: Activities and associated data concerning the command and control of operations that spans, impacts, or can be used by any and every organization within the U.S. Department of Defense.

Edge Innovation: In this report, we use the term *edge innovation* to describe the associated concepts of data accessibility, service composability, data fusion and collaboration within and among activities working together to meet mission requirements. Edge innovation makes the following possible:

> *Within and among activities, lightweight engineering support detachments (developers) team with operators to innovate new data sharing capabilities on demand. As potentially useful information resources are discovered on networks or as requirements for new information products emerge in the operational setting, engineers and operators collaborate on-site and virtually to compose new services and/or enhance the production and consumption capabilities of existing services. Developers access C2 Core capabilities available on the GIG to create the required shared information packages, including additional vocabulary and any needed mediation. Fast-paced T&E is carried out over the network with online assistance from Test Centers. New data services, products and artifacts are then registered so that they can be discovered and exploited by others.*

Federation: In the context of this study, a federation is group of cooperating services (federates) that interact on a network to support one or more larger capabilities, functioning as a whole to achieve specific objectives. Federations can range from extremely tight to loose, but qualifying for the term means that each federate retains some autonomy. Rules for a tight federation may include a common object model and supporting run-time infrastructure. Messages and/or other data sharing transactions that enable the federate services to cooperate as well as sequencing and timing are also carefully defined. In a loose federation, factors may be less rigidly defined or even purposely variable and the federates often have primary purposes other than the specific federation objective.

Federated Development and Certification Environment (FDCE): A DoD-specific, distributed test environment sourced by multiple Agency and Service providers designed to enable the rapid development, test, certification, deployment and acceptance of new products and services. It consists of processes, tools, and a federated development and test infrastructure.

GIG: The Global Information Grid (GIG) is a construct that embraces the entirety of Defense information sharing capabilities. Not just communications, the GIG includes "computing systems and services, software (including applications), data, security services…" etc. "…provides interfaces to coalition, allied, and non-DoD users and systems…" The magnitude of the GIG has profound implications for the Department's "information" designers and implementers. Examples: Precision search capabilities that allow globally distributed users to rapidly pull what they want from ultra-voluminous and variable information enclaves are critical. Large-scale distribution and maintenance of heavy clients is problematic. Metadata maintenance and high volume transaction processing required for fine grain access controls may constitute unacceptable overhead.

Information (or Data) Sharing Package or Shared Information Package: An articulation of an information object to be shared that includes the data object(s) and associated representation information, along with identified or intended consumers and their lifecycle requirements. A shared information package constitutes the basis for run-time interoperability and information sharing in that it specifies for consumers (human and machine) precisely what information will be published and in what form using what vocabulary to a level of detail that enables machine processing.

Information Support Plan: Per the DoD Acquisition Guidebook, a living deliverable that matures in concert with program specificity, reflecting the associated program or organization's plan to accomplish the goals of the Net-Centric Data Strategy (NCSD). In addition, run-time specifics essential to lifecycle management of the identified run-time data assets must be identified and maintained pre- and post-MileStone (MS) C.

Interoperability Matrix: A matrix to support the development, evolution and use of complex, component-based software. Interoperability matrices depict system or service versions versus specific versions of the structures used to publish or consume data by each system/service. These data structures are composed of more primitive elements and

may be depicted in matrices to allow users to determine the composition of any given version and find matching versions of components in other data structures.

JC3IEDM (Joint C3 (Command, Control and Consultation) Information Exchange Data Model): A data exchange model managed by the Multinational Interoperability Programme. In Dec 2007, MIP stated that 24 nations actively participate, including the United States. The scope of "JC3IEDM is principally directed at producing a corporate view of the data that reflects the multinational military information exchange requirements for multiple echelons in land based wartime operations and crisis response operations (CRO) to include joint interfaces that support land operations. The data model is focused primarily on the information requirements that support the operations planning and execution activities of a military or civilian headquarters or a command post." Per MIP, edition 3.0 will comprise the technical content of STANAG 5525 (NATO Standardization Agreement of the IEDM). MIP characterizes the purpose of the effort as follows:

a. "A description of the common data in an overall model that contains all relevant data abstracted in a well-structured and normalized way, unambiguously reflecting their semantic meaning.
b. A base document that can be used as a reference for future amendments to the model.
c. A core upon which nations can base their own modelling efforts of chosen areas and onto which specialized area models can be attached or "hung."
d. A basic document that nations can use to present and validate functional data model views with their own specialist organizations.
e. A specification of the physical schema required for database implementation."

JTF-level C2: Activities and associated data concerning the command and control of operations that spans, impacts, and/or is used by Joint Task Force Commanders and all of their subordinates.

Joint C2 Conceptual Model and Joint C2 Vocabulary: A service that publishes descriptions of C2 entities and their interrelationships together with terms and definitions that express properties of those entities.

Lifecycle Support Agreement (or Policy): Documentation that standardizes product support policies for developers and users of software capabilities. Support agreements or policies indicate, for example, how many years of support for specific versions will be provided as well as circumstances under which such support can be extended. Also, the nature of support may be specified; for example, a software product may be accompanied by full blown 24x7 help desk services early in its lifecycle, while in maturity it may only require online self-help support.

Lifecycle Timeline: A depiction in days/months/years of a product or capability's evolution from development, through test and evaluation to initial operational capability

through various stages of full operational capability and into retirement where it will be phased out and wholly replaced.

Mediators: Transformation capabilities that convert data from a source format into a representation that a consuming capability can ingest and process correctly. Two fundamental processes underlie any mediator: 1st - data mapping that relates elements from the source to the destination and captures any transformation that must occur and 2nd - code generation that creates the actual transformation program. Mediation capabilities can be value added processes organic to data sources, built into data consumers, or operated as independent services.

Metadata Catalogs: A type of service that stores descriptive information (metadata) about logical and physical data items. The main function of these services is to support data integration, mediation and categorization activities during development, but run-time uses are also emerging. Many allow metadata managers and users to aggregate artifacts into collections and provide system-defined as well as user-defined attributes for items and collections they assemble. Some enable users to dynamically define and add metadata attributes and will also provide names of user-defined attributes. Today, most metadata catalogs are implemented to run on top of standard web services.

Metadata Environment (MDE): Services, tools and processes associated with exposing and managing the full life cycle of metadata and supporting the visibility, accessibility, and understandability of the content and capabilities it describes. As applied to C2, the C2ISF, Core C2 services, and C2-related data sources (authoritative and others) constitute the run-time MDE. The build-time MDE includes conceptual models and vocabularies, Core C2 Service specifications, schemas and other data sharing package components plus associated governance and lifecycle management repositories, toolsets and services (e.g., configuration management, release management and interoperability matrices). Maintained by various CC/S/A organizations.

Metadata Registry (MDR): The DoD Metadata Registry is a clearinghouse for storage of metadata schematic formats. The DoD Metadata Registry can be found at URL http://metadata.dod.mil. Registration of metadata (e.g., databases, data dictionary elements, XML schemas, components, segments, and etc.) is an important activity to support interoperability in a net-centric environment. COIs will register their metadata components in the DoD Metadata Registry. Registering metadata components in the DoD Metadata Registry supports many-to-many interoperability by providing system architects and developers with insight into existing data schemas that they can employ and extend. The requirement that extensible metadata be registered applies to the schema of the metadata, not the actual metadata information environment and drawing on capabilities that enable the efficient, timely, and effective command of forces and control of engagements.

Navigation and Organization: The orderly arrangement of entities by categorization and/or substantive relationships to facilitate human and machine user discover of needed data.

Net-centricity: A property of systems and organizations that measures how open they are to interacting with others across a network to accomplish their goals, how quickly they can adapt to support unanticipated interactions, and how much cost they are willing to bear in order to be able to do these things. Net-centricity brings two revolutionary aspects to DoD information systems: (1) The ability to communicate routinely across traditional system and organizational boundaries in an open-ended or "asymmetric" way. (2) Being able to do this dynamically, changing the interaction and its organizational scope at run-time rather than at system development time. Implications: Political/social dynamics of organizations and their supporting information technology systems change dramatically, challenging most existing information model assumptions and frames of reference. Net-centric architectures generally make information systems more autonomic and adaptive but also complex in terms of large scale, infinitely variable connections and dependencies.

Net-Centric Enterprise Services (NCES): The DoD's program to define, develop, integrate, field and operate enterprise-wide infrastructure services for all IT systems sourced by the Department.

Net-Enabled Command Capability (NECC): The DoD's principal command and control capability that will be accessible in a net-centric environment and focused on providing the commander with the data and information needed to make timely, effective and informed decisions. NECC draws from the C2 community to evolve current and provide new C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. Warfighters can rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely and effective command of forces and control of engagements.

Reference Data: Information about entities, activities and relationships that an enterprise manages in order to represent its business in code (e.g., country or postal codes, vehicle types, personnel specialties), or information that categorizes the enterprise's information. Reference data is frequently stored in database tables that are also called "domains" or "lookup tables."

Run-Time: The period of time when software is running in an operational environment (not development).

Service: (1) The organizational entity responsible for acquiring, provisioning and vetting the quality of an authoritative data source. (2) The run-time software mechanisms needed to operationally access (publish/discover/read/write/delete/tag) an authoritative data source. (3) The development-time software mechanisms needed to define and expose an authoritative data source.

Service Oriented: Characterized by on-demand services. Participants in a service-oriented architecture make their resources available by publishing information in structured formats that describe their capabilities and how to access them. Other participants can discover and request those services on demand, but have no power to modify their makeup (other than by feeding back suggestions), ensuring their capabilities

always remain available to other participants. This loosely coupled, on-demand assembly of resources has the advantage of being highly adaptable to change. Implications: User populations may expand dramatically to include rapid incorporation of unforeseen applications and data sources. This impacts the nature of, timing of, and planning for upgrades.

Specific Extensions from the UCore: Schema components and vocabulary appended to the UCore as required, providing the ability to share more data within the C2 community. C2-Specific Extensions from UCore would be under configuration management of the C2 CPM in cooperation with the C2 community.

Universal Core (UCore): An approach for representing a few elements of information that are common to many environments in DoD and the IC. The initial release of UCore covers the geospatial elements of "where" plus an absolute time and time period for "when." In addition, the UCore includes a standard for security markings and the Department's cataloging standard. UCore is designed to be extensible so that Communities of Interest (COIs) can add data that answers their specific needs, allowing them to focus on the development of high value, mission-specific data vocabularies. The current Department policy memorandum asserts that adopting UCore will provide the following benefits:

- Facilitating consistent understanding of a small number of the most commonly used elements in information exchanges;
- Enabling organizations and automated systems exchanging information to easily understand the unambiguous meaning of commonly used terms.

UCore 2.0 provides a messaging framework that includes a digest of elements and a means for representing COI data as structured extensions from UCore within the context of this framework.

Production viability, scalability and operational effectiveness of UCore in a major acquisition program are still being assessed.

Unanticipated Users: A key aspect of service orientation is the notion that service providers do not necessarily know who their service consumers will be prior to performing the service and will provide their services to anyone with authorized access. Typically service providers will publish descriptions of service offerings and associated usage conditions or caveats to make them discoverable by potential customers (See DDMS). In essence, this activity constitutes a unilateral contract offering on the part of service providers, a contract that is closed when a service consumer accepts the pre-published terms for a given service and access is granted. Implications: Unanticipated users create uncertainty as to consumer population size and the nature of service/product usage.

Vocabulary/Terminology/Ontologies: an aggregation (usually a selected list) of words and phrases, which are used to tag and organize units of information so that they may be more easily retrieved by a search. Controlled ensure that each concept is described using

only one authorized term and each authorized term in the controlled vocabulary describes only one concept. In short, controlled vocabularies reduce ambiguity inherent in normal human languages where the same concept can be given different names and ensure consistency.

Vocabulary Management (Dictionaries, Term Banks, Thesaurus, etc): In the context of this report, knowledge management systems that can be used on DoD networks both for managing taxonomies, thesauri, classification schemes, and to provide users with the capability to control files and indexes. Vocabulary Management capabilities will generally provide users with configurable record structures, Web based user interfaces for all editorial tasks, and web-based indexing tools that allow for easy searching and browsing.

Appendix B.
Baseline Technical Questions

These Baseline Technical Questions were used in the initial technical interchange meetings with selected SMEs.

Introduction to the Problem

Many operational decision makers and others in the DoD leadership believe that C2 suffers from a lack of interoperability among currently deployed information systems. A major concern is coalition data exchange, but interoperability issues also exist among Joint and Service C2 capabilities; i.e., data from one "system" cannot be reused by another without burdensome interchange agreements negotiated on a pair wise basis among PMs. Some propose to mandate a 'core set of interchange semantics' to facilitate C2 system data sharing. JFCOM advocates a set of about 100 classes (as defined by a UML class diagram and vetted among members of the MIP community) each with an appropriate set of attributes (properties, slots, etc.) and relationships to fulfill this role. Others agree that a core set of data structures or semantic structures of significantly smaller size (marginally more than UCore Version 2.0) might be useful, especially if harnessed to a procedural and governance regime that permits agile evolution. This latter group points to the use of XML oriented, implementation structures such as the Shared Situation Awareness Track Framework (SSATF) as a viable engineering approach. In either case, policy will be required to make the data interoperability improvement plan work, and new constructs for technical management as well as engineering infrastructure will have to be put in place.

Our requirement was to provide recommendations regarding policies with respect to data which will improve C2 operations especially in joint, interagency and coalition environments Guidelines for implementing these policies Technical management processes, procedures and infrastructures for carrying out these policies. A process plus some candidate information sets, mission threads and domains for use in verifying the efficacy, risks, return on investment (ROI) and affordability of the recommended policies

Accordingly, we need to ascertain:

1. Do participants agree that there is an interoperability problem? If so, what specifically are its technical and procedural characteristics?
2. Will additional policy assist in solving the problem or is a piecemeal solution through engineering coordination sufficient? Would some deregulation help?

3. Who should issue any required policy, and what are the lines of authority and accountability? How will decisions be made, and how success will be measured?
4. From the standpoints of both developers and users, does mandating a 'core set of interchange semantics' cure or reduce or have no effect on the problem? Would it add to costs or realize savings?
5. What does it mean to mandate a core data set; e.g., require services/systems to map to an ontology? Use a specific set of message formats? Employ a specific data base schema? Use standardized domain values?
6. What range of possible impacts do we anticipate if policies such as discussed here are implemented? What is the timing of anticipated effects? How might they be recognized?
7. What other kinds of engineering approaches to data might benefit C2 from the data interoperability/information sharing standpoint?
8. What semantic artifacts must be created and maintained to meaningfully share information in a net-centric environment? Who should be responsible for engineering and evolving them?
9. How do we capture and measure consumer usage of and demand for the diversity of C2 data sets? How could the community use such metrics to drive a healthy evolution of data across the C2 environment? Who could use such metrics and what for?
10. Responsive engineering requires ongoing agreement with warrior and warrior support customers about needs. How can the process for aggregating capability requirements and engaging engineers to provide solutions be improved? How should responsibilities in this process be divided (where does requirements end and engineering begin)?
11. How do we leverage and/or accommodate evolving commercial standards and other government standards? From a policy standpoint? From a technical standpoint?

Appendix C.
C2 Roles and Responsibilities for Data

NII	C2 CPM	CC/S/A	Component PEO/PM	Infrastructure Provider
Develop, publish, maintain data policies and framework (5100.30)	Develop, publish, maintain CC needs based on operational metrics	Share operational metrics for analytics purposes	Use scalable, operational data stores w/ built-in metrics	Orchestrate distributed technical mgt (CM) of Joint shared information packages
Review metrics/trends for compliance, progress, results	Prioritize, on behalf of CCs, shared information packages	Publish ongoing data needs, C2 service improvements & priorities info	Participate in Joint shared information package CM process	Publish information sharing developmental status & metrics
Scale delegated authorities based on operational metrics (e.g.,. reputation)	Publish & maintain transitional interoperability tracking devices (interoperability matrices)	Actively participate in product, service development and integration	Publish & maintain transitional interoperability tracking devices (interoperability matrices)	Develop & operate selected data sharing infrastructure services
Use resources to support enforcement	Coordinate w/ "neighbor" portfolios	Work up operational IT capability packages (ensuring required interoperability)		Actively participate in data sharing product, service development and integration
	Define, report, and forecast operational metrics			Provide robust Metadata Environment (MDE), to include federation ability
	Establish and enforce data standards for C2			
	Coordinate testing (data, data services) and CM data artifacts			
	Support and track COIs and manage artifacts			
	Define C2 Core life cycle management processes.			

NII	C2 CPM	CC/S/A	Component PEO/PM	Infrastructure Provider
	Assign C2 Core life cycle artifact and process responsibilities.			

Appendix D.
Additional Notes

Summary IAT Findings

- Information Age C2 participants, behaviors and relationships are constantly shifting
- NGOs and loosely coupled coalition partners are often primary players in the mission space
- Social and cultural factors are often as important as geographical and material factors in situational awareness
- Missions evolve quickly (e.g., OIF went from Conventional War to Stability Operations to Counter-Insurgency)
- Commanders need to be able to reconfigure information sources and processes "on the fly" to maintain situational awareness
- Information and the supporting IT are key parts of the weapon suite
- Traditional systems, with embedded data, have engineering and programmatic tails which are not responsive to the current operational environment
- Data and tools for data discovery, access, understanding and use must be available in theater.
- Parts of the C2 community have been foundational in establishing a government-wide understanding that data sharing activities must concentrate on the operational run-time. DoD representatives to the UCore initiative have contributed greatly to the initiative and to DoD's understanding of the implications of NCDS.
- The C2 CPM, by developing a strawman definition of C2 Core (hereafter referred to as the JFCOM-defined C2 Core), has catalyzed an important and far-reaching discussion essential to NCDS success.
- A number of necessary, but insufficient, components to support C2 data sharing exist:
    - UCore (Version 2.0)
    - MDR
    - JFCOM-defined C2 Core vocabulary (to be modified by UCore)
    - DDMS

- The C2 community has actual consumption experience with several data service offerings (e.g., I3)
- COI and Component PEO/PM activities have identified gaps in proffered data and data services to support C2.
- Net-centricity and *edge innovation* are predicated on publish and subscribe data services (not point-to-point interfaces) that are reusable in multiple contexts (anticipated and unanticipated).
- Data sharing process and artifact definitions, along with associated concepts, are ill defined, leading to massive miscommunication and resulting in limited progress in addressing NCDS goals within the C2 community.
- Current JFCOM-defined C2 Core is insufficiently scoped to achieve NCDS goals, including edge interoperability.
- There are no concerted community efforts to define the physical data services required by every command to support C2.
- The C2 CPM has taken a leadership position in overall portfolio management, in spite of the immaturity of needed support structures and competing and overlapping guidance documents.
- A great deal of analysis has been performed based on JCIDS and the associated UJTLs to define common operational process needs for a typical symmetric JTF kinetic fight. As a result, detailed data and service needs have been identified.
- More and better operational data is being collected and exposed than ever before, particularly through embedded observers who generate a plethora of observations and lessons learned documentation.
- Certain COIs of interest to the C2 community have identified and begun to work on operationally derived data sharing requirements.
- The Federated Development and Certification Environment (FDCE) represents a positive and essential step in support of NCDS goals. In particular, the FDCE offers an opportunity to make the development process far more transparent so that potential users can identify a capability well in advance of IOC and begin to make technical adjustments. FDCE may also increase the confidence of potential users that fielding risks are acceptable.
- Overall reconciliation and clean up of competing and duplicative messaging standards has been undertaken, with "classical" allied participation. Properly leveraged, common data vocabularies and taxonomies could support NCDS goals and improve edge interoperability.
- C2 is much broader than what is required to support a typical symmetric JTF kinetic fight. In fact, a number of reports clearly identify that the bulk of current operational C2 decisions are not kinetic in nature and are not made at the JTF level, but rather, at the squad and platoon level. The existing analytical work should clearly be leveraged as context for that subset of data

and associated services to which it applies, but it reflects only a small (and, perhaps, not most important) part of the current data sharing problem set.

- The IT provisioning chain continues to be fractured along functional responsibility lines, resulting in a lack of common decision criteria and vision among key contributors. Consequently there is lack of understanding that configuration management must span the complete data or data service lifecycle, from needs definition through operational run-time. The end-of-life decision is one of the most serious, potentially impacting fielded capabilities, especially where there has been extensive re-use.
- The C2 community is not leveraging operational use data in any consistent manner. Some of this is, in part, due to differences in the collection and reporting mechanisms employed. Regardless of format and content, much of this valuable field reporting isn't applied to prioritizing implementation.
- Measured operational use data is essential to manage the IT provisioning chain effectively in a net-centric environment. This is standard commercial practice; it provides a means of prioritizing IT investment, as well as informing key decisions impacting the complete IT lifecycle. Only ongoing user metrics collection, combined with trending and analytics, can lead to understanding of actual operational needs. This lesson, and associated underpinnings (e.g., focus, process, technology), is completely absent in current NCDS activities.
- In addition to the definitional problems identified in Finding 2, mandates for compliance and/or conformance are insufficiently specific to assure NCDS goals are achieved.
- Mainstream DoD IT provisioning chain participants and processes continue to employ "old think" in relation to NCDS. This will result in proscribing the implementation and rendering, over time, such participants irrelevant unless and until they viscerally understand and implement required changes. Two areas where this manifests itself most visibly today are in CM and testing approaches.
- Efficacy and performance of COIs is inconsistent. For those COIs which are addressing compelling data sharing requirements, there is no over-arching C2 structure to capture and leverage their work other than registration of metadata products (if any) in the MDR.
- Although overarching messaging standardization work is ongoing, it exists in parallel to every competing subsetted messaging standard and associated governance structures and processes. There appears to be no concerted effort to reconcile or collapse competing or duplicative messaging activities.
- The IAT performed an analysis that compared current "uber messaging" signatories and implementers to coalition partners in Afghanistan and Iraq. Unfortunately, only 30% of the countries participating in current operations in those two AORs are also involved in this "overarching" messaging consolidation activity. Further, DoD messaging activities, in general, do not

encourage nor allow for participation by NGOs, which figure heavily in all stabilization operations.

- C2 discussions are conflating a number of related, but different, concepts (e.g., DoD-wide C2, JTF-level C2, NECC, COI)
- Conflicting and/or confusing policies exist and/or are being implemented (e.g., portfolio management)
- Goals and priorities with respect to data are not clear within the C2 community and are not obviously aligned with DoD Net-Centric Data Strategy

Finding 2: UCore and a re-defined C2 Core could enable community-wide data sharing. C2 should leverage UCore and C2 Core, where C2 Core consists of: 1) a C2 Information Sharing Framework to support C2 IT development and operations; 2) a Joint C2 Conceptual Model and Joint C2 Vocabulary to provide context and the current C2 vocabulary, 3) C2-Specific Extensions from UCore to facilitate data sharing within the C2 community; and 4) C2 Core Service Specifications for C2-specific services.

IAT observations:

- Parts of the C2 community have been building government-wide understanding that data sharing activities must focus on run-time. DoD representatives to the UCore initiative have contributed greatly to the initiative and to DoD's understanding of the implications of NCDS
- By developing a strawman definition of C2 Core (hereafter referred to as the JFCOM-defined C2 Core), the C2 CPM has catalyzed an important and far-reaching discussion essential to NCDS success
- A number of necessary, but insufficient, components for an operationally focused set of data and data services to support C2 exist:
  - UCore (Version 2.0)
  - Metadata Registry (MDR)
  - JFCOM-defined C2 Core vocabulary (to be modified by UCore)
  - DoD Discovery Metadata Specification (DDMS)
- The C2 community has actual consumption experience with several data service offerings (e.g., I3)
- COI and Component PEO/PM activities have identified gaps in proffered data and data services to support C2.

As an overall observation, the DoD, including the C2 community, continues to iterate on incremental improvements in classical interoperability (point-to-point) thinking, rather than re-evaluating the demands of net-centricity and the resulting implications. Emphasis must transition to the run-time and operational impact of data sharing. IAT findings include:

- Net-centricity and *edge innovation* are predicated on publish and subscribe data services (not point-to-point interfaces) that are reusable in multiple contexts (anticipated and unanticipated)
- Data sharing process and artifact definitions, along with associated concepts, are ill defined, leading to miscommunications and limited progress in addressing NCDS goals within the C2 community
- Current JFCOM-defined C2 Core is insufficiently scoped to achieve NCDS goals, including edge interoperability
- There are no concerted community efforts to define the run-time data services required by every command to support C2.

Net-centricity and *edge innovation* are predicated on publish and subscribe data services (vice point-to-point interfaces), which are reusable in multiple contexts both anticipated and unanticipated. In particular, C2 edge innovation requires a set of foundational components comprised of at least the following:

- A run-time production infrastructure and metadata environment
- A development environment smoothly coupled with the production infrastructure
- Shared services
- Agreements on published vocabularies supported by published information sources
- Agreements on published concepts needed to describe objects and operations in the mission space and how to add new concepts and descriptions
- Agreements on published formats and data structures for publishing information via shared services.

A production environment is required to identify, describe and locate available data and services for potential users. This environment should include registries of services, catalogs of instance data, and registries of structural descriptions of data and vocabularies. Tools should be available to ease the burden of creating and managing metadata used in operating the run-time production environment.

Although rudimentary, a number of necessary but insufficient components for a suite of data innovation services exist today. These include the UCore, the DoD Metadata Registry (MDR) and Services Registry, some candidates for a baseline C2 Core common vocabulary and conceptual model (JC3IEDM sections).

Although the C2 community has significant operational experience with managing and consuming data service or service-like offerings (e.g., I3, IBS), there appears to be no concerted community effort to define a core set of physical data services required for or common to all C2 operations centers. The IAT believes that such a core can be defined, possibly via a standard core and a “core-lite” for smaller disadvantaged centers.

The foundational C2 Core should be deployed as an evolving set of services, specifications, artifacts and processes that enable visibility, accessibility and understandability of data to support command and control of operations.

Populating and Maintaining the C2 Core

The initial C2 Core baseline and all subsequent versions should consist of C2-specific data and associated data services that (1) are nominated by a COI of interest to the C2 community, (2) demonstrably address one or more specific and current operational data problems, and (3) are proven extensible to the Version 2.0. All corresponding artifacts will be published in the DoD MDR C2 area and the NCES Service Registry.

The C2 CPM should establish needed governance and management processes using existing enterprise and C2-specific services. (Appendix C: C2 Roles and Responsibilities)

Constraints on Policy Documentation

The following constraints on policy documentation are recommended:

- Resist the temptation to focus on new programs. Address both current systems and future applications/services and how to move from one to the other (few "green field" opportunities)
- Avoid specifying technology
- Limit policy to "public" interfaces; do not engage on internal representations and functionality
- Break out of the acquisition stovepipe. The gap between day-to-day operations and development must be closed to realize agility
- Formalize and carefully delineate responsibilities, but emphasize collaboration across organizational boundaries
- Define measures of success (metrics and anecdotal feedback from users). Keep it simple, particularly in the initial stages; satisfied users vote with their keyboards. Meeting the basic NCDS visibility goal can be verified by simple pass-fail discovery checks at readily available NIPR/SIPRNet terminals
- Despite high level resistance to policy turbulence, respond to "conditions on the ground" vice hard-wired schedules
- Make it clear that foot-dragging is unacceptable. If given top-level cover, any program can and should initiate some actions that positively impact warfighter data sharing in the near term by redirecting available implementation resources.

C2 CPM Policy Guidance

- Establish and maintain operational focus. In order to fulfill C2 CPM responsibilities, the C2 CPM must be clear on operational priorities, their operational impact, and how these tie to any IT activity proposed in their support. This requires that the C2 CPM articulate goals, in concert with operators, which target specific effects. Identify end user best value. The C2 CPM must be sufficiently aware of acquisition and technical limits to identify and prioritize, on behalf of the C2 end user, data and service delivery that is highly valuable to that end user.
- Establish current IT and Acquisition Situational Awareness for the C2 community. (See Appendix E.)
- The C2 CPM should maintain a federated data and service operations catalog that (1) reflects current data and service fielding plans and (2) provides visibility into unit-level data exchange disconnects. By federating constituent Component PM and PEO Interoperability Matrices by release, the C2 CPM will be uniquely positioned to identify and address, a priori, such disconnects. Eventually, this federation should extend to key "neighbor" portfolios, which represent heavy partners from a provider or consumer standpoint. For example, as Intelligence is a key enabler of C2, certain Component PMs and PEOs in that portfolio likely represent key federation partners for tracking data exchange capabilities.
- Establish an open, participatory C2 Core management process. The C2 CPM and artifact publishers should jointly establish an open, participatory process to (1) populate and maintain C2 Core, (2) certify extensibility, and (3) lifecycle-manage C2-Specific Extensions to UCore Version 2.0. Generally, UCore extension publishers should maintain direct CM over the artifacts they create with the C2 CPM orchestrating their efforts. Where necessary, the C2 CPM will engage with selected publishers to address continued use of those artifacts lacking certification within the C2 community. Since configuration management of the C2 Core specifications and artifacts must necessarily be decentralized, careful consideration to this is warranted in the initial population process.
- Communicate operational goals relentlessly. Finally, and most importantly, the C2 CPM should relentlessly communicate the vision and goals for IT support to operators in both acquisition and operationally terms. The C2 CPM should collect, analyze and publish operational metrics and associated trends and let those numbers speak to the C2 constituency. This will allow the C2 CPM to stay "above the fray" in terms of identifying or calling out "poor" suppliers. The C2 CPM should absolutely be the first and most vocal proponent of the current plan. If there are challenges, those should be worked outside of public forums. The C2 CPM represents the C2 community to the DoD, as well as to the broader world. They must improve or uphold the C2 community reputation as a principal responsibility.

C2 Core Implementation Guidance

Shared Information Packages. Properly implemented, Shared Information Packages constitute the basis for run-time interoperability and information sharing; that is, they are available both semantically and syntactically (e.g. data in context). The following recommendations constitute a basis for defining and describing shared information packages, but may not be complete. At a minimum, the IAT recommends:

- Specifications for how to construct an XML package of shared information with a minimum set of common information including where, when, discovery (DDMS) and what
- Shared Information Packages may be extended by COIs and Portfolios, however the extensions should be exposed and managed at appropriate levels.

Appendix E.
Acquisition Situational Awareness

Introduction

This paper provides recommendations for data policy and implementation for the C2 community, including recommendations for strengthening and expediting linkages between acquisition and operations to maximize operational responsiveness. One way of doing this to apply net-centric concepts within acquisition process itself. This Appendix proposes an information environment for acquisition situation awareness.

Taking lessons learned from the World Wide Web, the DoD Net-Centric Data Strategy envisions a national security information sharing environment where functionality and content-providing capabilities on the Department's networks are packaged and operated as services. These services are advertised by providers, and then discovered and used by consumers. In the commercial analog of this vision, competitive Internet Service Providers (ISPs) have determined that delivering high quality functionality and performance to customers means continuously monitoring, measuring, and assessing the response to and the responsiveness of their offerings. Service capabilities in the global Web-based information marketplace are continually being enhanced by the individual organizations that operate them as justified by the observed return on investment (ROI).

Information Age managers recognize that the ROI of a service cannot be reliably estimated in the absence of quantifiable observations. Every business unit in a successful enterprise needs to demonstrate its worth not only through collecting user testimonials but also through a steady stream of hard empirical data from instrumentation. With its multi-billion dollar IT investments, DoD is certainly no exception to this pattern. Moreover, the data strategy goals require not only that this stream of empirical data be generated but also that it be widely available in near real time, particularly to support agility. In this context, agility means being able to rapidly upgrade the functionality and content of existing information services or to rapidly augment the Department's capability with wholly new services. Pursuing either of those activities means engaging in the DoD acquisition process. The data strategy tells us that the current process must be transformed to become net-centric.

Acquisition Process Transparency: Providing Acquisition Situation Awareness

While traditional acquisition rules and their legal underpinnings remain in place, initial net-centric acquisition capabilities should be designed to enhance effectiveness of the "Big A" acquisition process (acquisition management, JCIDS, and PPBE). However, an

additional and distinguishing feature of net-centric acquisition is its strong emphasis on providing a near-real time picture of the changing *as built* baseline capability; i.e., the state of operational networks together with the functionality and content-producing capabilities that are currently deployed. This is essentially an information management-oriented user-defined operational picture. Transparency into these activities, the changing *as built* and the planned/developing *to be* capabilities can be supplied by an Acquisition Situation Awareness (ASA) service that is made widely visible and accessible within major network enclaves as shown in Figure 2.

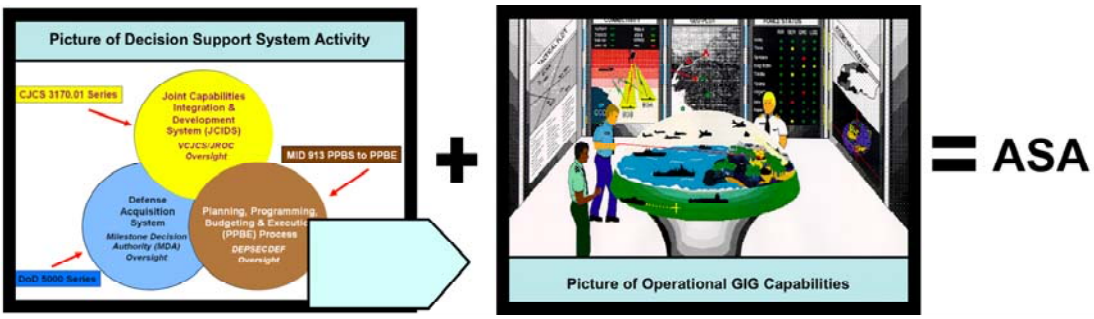

Figure 2. Fusing the Acquisition Situation Awareness Picture

A major thrust of net-centric "Big A" acquisition must be to improve data transparency to DoD personnel charged with oversight. Streams of data reflecting current activity and status of information within the acquisition management, JCIDS, and PPBE processes must be identified and evolved, and then the output must be published and presented for enterprise decision support. Figure 3 shows the proposed net-centric acquisition environment.

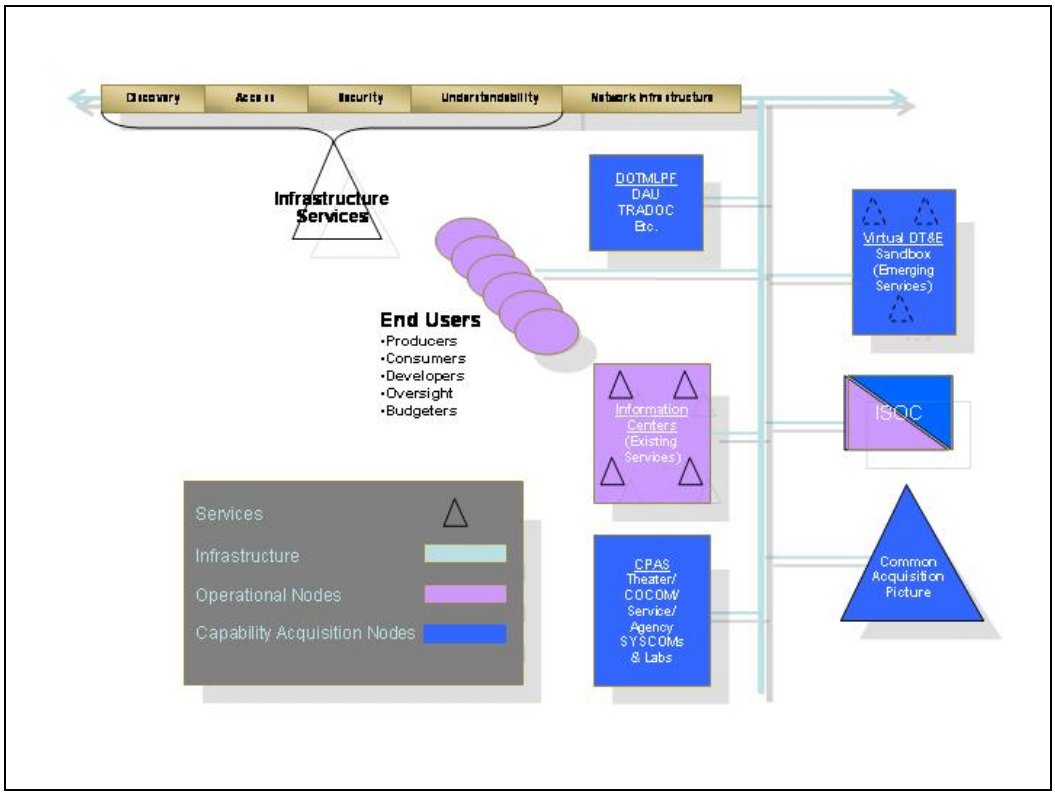

Figure 3. Net-Centric Acquisition Environment

The organizational roles and responsibilities depicted in Figure include:

- **Capability Provisioning Activities (CPAs)**. COCOM, Service, and Agency development organizations, system commands, labs, and other research facilities both in CONUS and in theater must engage in collaborative engineering and self-synchronized technical acquisition activities.
- **Operational Information Centers**. Joint and Service command and intelligence centers at the national level and within COCOMs plus operations and intelligence centers or cells extending down to wing, ship, and battalion levels and below are the backbone of warfighter information management, including combat support logistics, planning, and public affairs. These centers have always engaged in substantial information sharing up and down the chain of command.
- **DOTMLPF Activities**. Few capability gaps require a material solution alone. Most involve some organizational or procedural modifications. The JCIDS recognizes that closing a capability gap may require either a materiel or non-materiel solution and in most cases both.
- **Information Sharing Operations Center (ISOC)**. ISOC support functions include:

- Provide situational awareness (SA) of content and services available to support DoD and other national security users and to coordinate resolution of infrastructure-related issues that impact information sharing
- Provide near real time infrastructure support to:
    - Operate and manage the minimal set of core enterprise services necessary for information sharing (provided through GISMC)
    - Monitor and maintain SA of enterprise services and associated communications infrastructure (communications links, servers, databases, applications, etc.)
    - Report service denials and degradations
    - Ensure timely and accurate trouble ticketing of key information-sharing components
- Periodically collect statistics on the usage and health and status of services and data, which are provided to the information broker for analysis and to information producers
- Maintain a current information sharing picture that reflects the status of publishing, consuming, and searching by:
    - Collecting metrics on usage (type and quantity for both publishing and consuming) and user feedback
    - Maintaining and publishing inventories of Web sites, services, etc.
    - Administering and managing the COI directory and enterprise catalog
    - Maintaining standards for publishing COI data
    - Conducting periodic drill-down searches to discover and catalog restricted GIG data sources
- Maintain robust feedback mechanisms responsive to user input by:
    - Providing quality assurance for published information resource offerings comparing advertised capabilities with observed capabilities
    - Maintaining enterprise-level bulletin boards (e.g., wikis, blogs) and provide enterprise-level user forum functions (e.g., user groups, discussion forums)
    - Analyzing information-sharing trends to identify challenges and key information assets
    - Facilitating the sharing of key information assets through proactive engagements with information producers
    - Providing input to portfolio managers and other decision makers
    - Spotlighting emerging groups (users with similar interests) to facilitate COI creation/convergence and provide guidance on how to form COIs

- Analyze information and services activities on the infrastructure by:
    - Conducting after-action and lesson-learned analyses of information-sharing outages, failed discoveries, and denials of service
    - Coordinating with NetOps entities on bandwidth/transport demand and reallocation to support information-sharing surges/outages
    - Coordinating domain name server load-balancing actions
    - Coordinating with NCES Content Staging Services to capture and stage critical data
- Establish and maintain standards for posting and subscribing to Acquisition Situation Awareness data in accordance with the data strategy
- Help warfighters, intelligence analysts, and business personnel:
    - Know what information resources are available to them
    - Find specific information crucial to their missions
    - Provide information to others who may need it
    - Adjust information support arrangements rapidly
    - Determine the quality of published information
    - Measure the value of their information investments
    - Interact directly with responsive information providers
    - Rapidly incorporate new information sources into operations

The FDCE Sandbox: Federated Acquisition Organizations, Processes and Capabilities

The Federated Development Certification Environment (FDCE) was conceived as virtual capability within the Global Information Grid (GIG) intended to address the challenges associated with developing and certifying net-centric services. Its purpose is to provide the policies, processes, and infrastructure that allow services to be progressively refined, tested, evaluated, and certified in increasingly rigorous situations leading to an operational deployment. The environment is *federated*, emphasizing that it is not used, controlled, or operated by a single organization. Rather, it is a virtual collaborative environment made up of the appropriate service providers, testers, evaluators, certifiers, DOTMLPF experts, and operators from across DoD and beyond. The FDCE is intended to facilitate the ongoing interaction and collaboration of these organizations throughout the entire development and certification process, extended into formulating capability enhancements.

To concurrently address all aspects of development and certification, the FDCE must support multiple levels of maturity within the service building process. The environment

should consist of at least three maturity enclaves in addition to the operational enclave (see Figure 4).

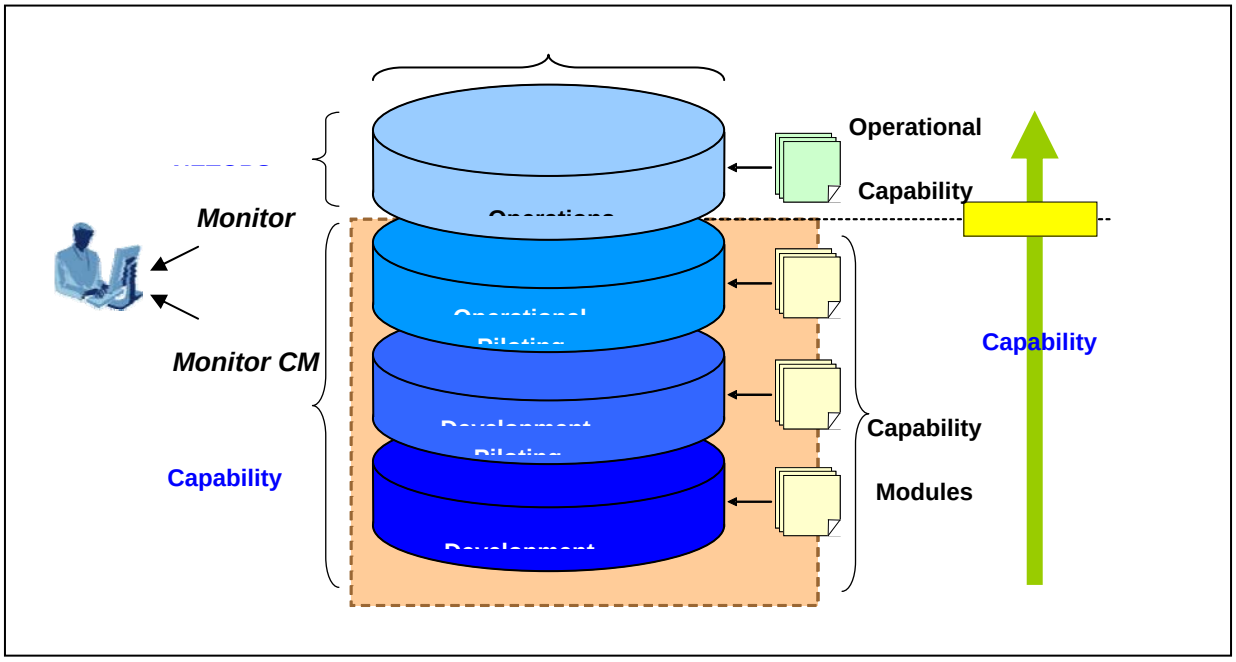

Figure 4. Federated Development and Certification Environment Enclaves

The FDCE enclaves will support the full range of development and certification functions from initial development through operations. Each enclave in the FDCE is intended to support a different set of development and certification activities. Services will start at the Development Enclave and progressively work their way through each enclave, eventually making it to the Operations Enclave. Each enclave will have entry criteria that are appropriate for the activities associated with that enclave's level of maturity.

- **Development Enclave**. The Development Enclave is the entry point for service providers as they begin developing and testing their new software services. It is intended to facilitate the development and testing of individual services by making it as easy as possible to play. A key objective for the Development Enclave is to have a low cost of entry. To facilitate this goal, the Development Enclave will operate primarily at the unclassified level and will minimize the certification and configuration management requirements to participate.
- **Development Piloting Enclave**. The Development Piloting Enclave focuses on (1) service-to-service integration into mission threads and (2) performance testing of how well services are meeting their service level agreements. At this level, a much greater degree of rigor is introduced into the process as compared to the Development Enclave to enable more controlled evaluations of service performance under realistic loading conditions. The Development Piloting Enclave will include both classified and unclassified components.

- **Operational Piloting Enclave**. The Operational Piloting Enclave is focused on the operational testing of individual services and the evaluation of services in end-to-end mission threads. Services that reach this enclave will have demonstrated strong evidence of their ability to meet their technical performance objectives as part of Development Piloting activities. Services in the Operational Piloting Enclave will have the ability to access to real-world data to support operational evaluation.

In a fully developed and fully operational FDCE, developers will have numerous versions of their services registered in multiple enclaves. The management of a single service within the FDCE will quickly become more complex than simply walking your service from development to operations in four sequential steps. Effectively managing progression and digression of services within the FDCE, as well as handling multiple service versions, will be an important issue for the FDCE to address. Service and metadata registries will be tied in to support these FDCE needs and to ensure that all registration required for visibility into the status and the substance of important issues has in fact occurred.

The FDCE will publish information concerning capabilities under development on a regular basis with spot reports concerning movements from one enclave to the next and achievement of certifications. Thus, the FDCE would become the primary means of providing visibility into the state of developing information capabilities.

To achieve a *net-ready* certification, services will need to be certified against a number of different categories of *net-ready* criteria. Meeting these criteria not only reflects a new capability's state but also assures that registration of required metadata has occurred to support discovery of detailed ASA information. The full range of appropriate criteria categories will evolve; however, the following are expected to be included in the first version of the net-ready certification set:

- **Registration**. Certifies that services are registered in a manner required to ensure visibility, accessibility, understandability and other data strategy goals
- **Community Independent Security**. Certifies that services are compliant with the core enterprise security model.
- **Configuration Management**. Certifies that services conform to the configuration management processes associated with the enclave.
- **ESM Enabled**. Certifies that services are compliant with the reporting requirements of enterprise service management (ESM) services. This capability is required to support many of the reporting requirements in the categories below.
- **Availability Guarantees**. Certifies that services have established minimum availability thresholds and are able to meet them.
- **Response Time Guarantees**. Certifies that services have established minimum performance thresholds on the response time of their service and that they are able to meet them.

- **Reliability/Survivability Guarantees**. Certifies that services have established minimum reliability/survivability thresholds and are able to meet them.
- **NetOps Ready**. Certifies that services have provided mechanisms for supporting enterprise NetOps (network operations) activities.
- **On Line Help**. Certifies that services provide on-line help (either built in or via help desk).
- **Lifecycle Commitments**. Certifies that a service provider has committed to keep the service operational for a specified period of time.

Registration of this information as capabilities progress through the various certification enclaves is central to generating the ASA. The ASA will enable developers, oversight officials, operators, and future users to determine the precise status of new capability initiatives and assessments of IOC functionality, timing, and associated risks. This information is vital to determining whether capabilities in the development pipeline are adequate to answer known user requirements or whether additional action is required.

Measuring Net-Centric Capabilities

A wide variety of measurements and assessments that can be undertaken to monitor both developing and operational capabilities on large-scale networks. These can be very broad measurements, applying to the traffic patterns and usage of the Internet as a whole; or they can apply specifically to an organization's intranet infrastructure, which might include the network connections, cables, workstation computers, servers (computers used to host Web sites, shared software applications, and e-mail systems), and Web services. Knowledge of the degree to which operational capabilities are satisfying user needs is key to planning and executing enhancements.

Internet metrics refers broadly to any number of networked capability behaviors that can be measured or presented in a statistical format, including online advertising industry revenue reports and projections, trends about the preferences of Web site users, or other statistics about the Internet economy. Global Internet metrics also apply to different technical aspects of the Internet's infrastructure, including the miles of cable and wireless capabilities that connect the world’s computers, routers that relay information among specific devices on the Internet, and different ISPs.

Satisfaction of customer needs is the “bottom line” objective for both industry and government operations (albeit the endgame being dollars in one case and successful public service in the other). Customers demonstrate their satisfaction through usage of Web capabilities. There are three principle ways to measure Internet usage by humans:

1. The behavior of volunteers or test users can be measured at computers installed in an information center expressly to gather metrics (user-centric)
2. Marketers can monitor how real-world visitors interact with a specific Web site’s capabilities (site-centric).

3. Data can be collected directly from ISP networks (network-centric) using such capabilities as Web site usage log analysis.

The range of industry standard usage metrics related to monitoring Web sites includes counting page requests, visits and average visit length, and these can be combined with other factors such as user demographic and lifestyle information across thousands of Web sites that are reported on every day. In today's commercial operations, the sample size of data analyzed is generally in the 10s of millions range. Methods are also available to gain insight into the search terms used to find thousands of sites as well as click-stream reports for analyzing the movements of users among sites.

These methods are aimed at providing operations managers, their engineering support, and their higher-level executive oversight with answers to questions like:

- Who is visiting the Web site and how did they find it?
- How many page views, visits (sessions) and visitors are coming on a daily, weekly, monthly, quarterly or yearly basis?
- What content, products, and services do our visitors prefer?
- How many visitors return to the Web site and how often?
- What kind of search engine do they use?
- What other kinds of technology do visitors have to exploit the Web site?
- How much time do they spent on the Web site?
- How do visitors use the information they collect from the Web site?

When these kinds of data are collected and analyzed over time, vital information on the effectiveness of transformation or other behavior change initiatives can be substantiated. Real increases in information sharing can be documented to the extent of revealing specific content, for example, through site visits and hits on specific offerings within a site. End point censuses can show that a given intranet is rich or barren and detect that its content is blossoming.

Internet-style metrics play a number of critical roles at various organizational levels. Just as companies use Internet metrics to measure, monitor, and report on their financial performance, successful organizations also take steps to measure the IT capabilities of their business activities so that they can be improved. This involves monitoring performance and statistics at the user (client) level, on the back end (different computer systems and databases), and at a level in between these that includes such technicalities as network performance and servers. These kinds of metrics and other metadata are crucial to speed and precision in acquiring capability enhancements that answer user needs.

Effective Acquisition Management and Oversight *Requires* Transparency

High-level DoD overseers are charged with ensuring that the Department invests its IT dollars smartly. To take a Net-Centric Data Strategy example, they might pose questions

regarding the magnitude of programs' investments in schema for data sharing and whether they are justified. One of the few operational Enterprise Services available today is the DoD Metadata Registry (MDR). There are about 100,000 metadata components registered in the MDR. Many of these are odds and ends including elements and valid values, but about 4000 are actually XML (Extensible Markup Language) schemas that developers can download and use to post information payloads.

Assuming for illustration that each of these schemas represents a $250,000 investment (one engineering staff year), then those 4000 schema represent $1B worth of metadata engineering. The products of this investment are visible, accessible and understandable to their management, users and oversight only because they are registered in the MDR! If there were no MDR, no estimate would be available of DoD's investment in XML schema within the right order of magnitude. Additionally, MDR registration facilitates accountability by tracking who is responsible for each schema.

No one knows how many schema are actually required by the Department because there is no empirical information to tell us what capabilities are riding on DoD networks, what transactions are actually taking place among them, the substance of those transactions, and what the shifting information sharing shortfall is at any given point in time. Without visibility into the operational *as built* architecture, the XML schema requirement could be 400, 4000, or 8000 or 80,000! No one knows! We can point to evidence that suggests the number may be quite large. For example, the Army Battle Command System maintains over 150 interfaces, each with a separate transaction format.

Some may question the amount of schema reuse, supposing that it should be greater than indicated and that the 4000 known schema are too many. That may or may not be true, but if the amount of reuse does prove to be too high, the reason will be inadequate oversight and ineffective management on the part of myriad PMs, engineers, and oversight officials. Of course, even a bad management assessment is hard to back up in the absence of facts. The Acquisition Situation Awareness environment is intended to make these facts visible, accessible, understandable, and trusted.

References

Documents

Net-Enabled Command Capabili*ty, Shared Situational Awareness Capability Definition Package* 1, 30 July 2007.

Net-Enabled Command Capability, S*hared Situational Awareness Capabi*lity Definition Package 2, 7 December 2007.

Net-Enabled Comm*and Capability, NECC Increment 1 Data* Architecture, V1.0, 2 November 2007.

Net-Enabled Command Capability, NECC Increment 1 Software Architecture, V1.0, 19 October 2007.

Net-Enabled Command Capability, Conte*xt Data Source Adapter* (CDSA) Specification, V2.0, 02 November 2007.

Net-Enabled Command Capability, Architecture Framework, V1.0, 31 January 2007.

Army and Marine Corps C2 SA Convergence Study, Interoperability Analysis Document, Version 2.0 Final, MITRE, March 2008.

Unite*d State*s Joint Forces Command, Joint Common System Function Lis*t, Increment 1, Version 0.5.0, Draft, 17 December 2007*.

*Unite*d States Joint Forces Command, NECC's Implementation of the DoD's Net-Centric Data Strategy, V1.0, 12 January 2007.

Draft Command and Control (C2) Capability Portfolio Manager (CPM) C2 Information Exchange Vocabularies Concept of Operations (CONOPS), July 2008.

Command & Control (C2) Core v1.0, DRAFT, Vision and Scope Document, C2 Capability Portfolio Manager (CPM), April 2008.

Overview of the C2 Core Data Model, Version 1.0 Draft, 31 March 2008.

Universal Core (UCore) Description and Implementation Guide (DIG), Version 2.0.0, DRAFT, 01 May 2008, UCore Development and Configuration Management Working Group.

C2 Data Framework Concept and Technical Guidance, Version 1.0, Originators: USJFCOM J87 Joint Data Strategy Division, C2 Data Framework Technical Working Group, March 27, 2008.

Army Net-Centric Data Strategy (ANCDS), Center of Excellence (CoE) charter, CIO/G-6, Creation Date: 19 July 2007, Version: 1.

Office of the Assistant Secretary of Defense, Networks & Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO), Department of Defense Command & Control Strategic Plan, Draft Version 0.99, 15 August 2008.

IBM Response to Request for Independent Assessment of the Command and Control (C2) Data Strategy, Paul Giangarra, IBM Distinguished Engineer, August 2008.

Net-Enabled Command Capability, Shared Situational Awareness Capability Definition Package 1, 30 July 2007.

Army Net-Centric Data Strategy, Data Reference Model, A White Paper, James Blalock, CIO/G-6 Technical Architecture Division, Architecture, Operations & Space Directorate, Jan C. O'Malley, ANCDS CoE in support of CIO/G-6, June 2008, Version 1.1.

Department of Defense Net-Centric Services Strategy for a Net-Centric, Service Oriented DoD Enterprise, May 4, 2007, Chief Information Officer.

Department of Defense Directive 7045.20, "Capability Portfolio Management," September 25, 2008.

Department of Defense Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005.

Department of Defense Instruction 8115.02, "Information Technology Portfolio Management," Implementation, October 30, 2006.

Department of Defense Directive 5000.1, "The Defense Acquisition System," May 12, 2003.

Department of Defense Instruction 5000.2, "Operation of the Defense Acquisition System," December 2, 2008.

Defense Acquisition Guidebook, http://akss.dau.mil/dag/

Department of Defense Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004.

Draft Net-Enabled Command Capability (NECC), Increment 1, Capability Development Document (CDD), Change 1 Annex, 10 July 2008.

United States Joint Forces Command, Joint Common System Function List, Increment 1, Version 0.5.0, Draft, 17 December 2007.

DRAFT C2 CPM Data Standards and Standards Implementation Validation CONOPS, 2008.

DRAFT Charter for Command and Control Portfolio Data Strategy, Version 2.0, 16 July 2008.

C2_NECC Data Needs Matrix, NECC Program Office, 18 September 2008.

Command and Control (C2) Portfolio Data Strategy Management, DRAFT, Configuration Management (CM) Plan v1.0.

Annex C, Model Working Group TOR, Net-Centric Enterprise Interoperability Working Group, DoD and France MOD for Research, Develop*ment, Testing and Evaluation Projects*.

*Our Contribution to Legitimat*e Iraqi Governance and Development, II MEF (Forward), *MNF-W OIF 06-08, 1 November 2006*.

Battle Command Software: Meeting the Commander's Needs, USAWC Strategy Research Project, LTC David M. Moore, USA, 15 March 2006.

Memos

Department of Navy Deputy Chief Information Officer Memo, Subject: Navy Enterprise Architecture and Data Strategy (NEADS) Policy, dated 6 April 07.

DISA Director's Memo to ASD (NII), Command and Control (C2) Data Dependencies, 4 June 2008.

Department of the Army Memo, Subject: Army Data Harmonization and Integration Working Group (ADHIWG) Charter, dated 17 August 2007.

DoD CIO Memo, Subject: DoD Net-Centric Data Strategy, dated May 9, 2003.

Joint Staff Memo, Subject: Net-Enabled Command Capability Increment One Capability Development Document, dated 16 July 2007.

Joint Forces Command Memo, Subject: Command and Control (C2) Vision, dated 7 May 2008.

MFR, Strike COI – Steering Committee Meeting, dated July 29, 2008.

MFR, Trip Report - Project Manager and TRADOC Capabilities Manager Battle Command Travel, 10 - 25 June 2007, dated 04 July 2007.

Site Visit Report, Marine Corps Tactics and Operations Group, 29 Palms, Maj Chris Beckford, MAGTF C2 Lead Systems Architect, 4 April 2008.

Meeting Minutes, US/France Data Experts Meeting, 24-25 September 2008.

Briefings

ITMC Background and Drivers, Dept of Navy, 2008.

Multilateral Interoperability Programme (MIP) and the C2 Core Data Exchange Standard, Mr. Stuart Whitehead, SES, Executive Director, USJFCOM Joint Capability, Development Directorate (J8).

C2 Data IPR for DCDR, USJFCOM, 09 June 2008Mr. Stuart Whitehead, Executive Director, USJFCOM Joint Capability Development Directorate (J8).

Net-Enabled Command Capability, Brig Gen Hoene, v9, 12 May 08.

C2 Core: US Army Analysis Evaluation Factors Discussion, July 2008.

Universal Core, Interagency Information Sharing Initiative, Presented to: Defense Science Board, 15 July 2008.

JC3IEDM SOA Pilot Iteration II CIO-G6, 30 July 08.

Overview of the JFCOM C2 Core, Gene Simaitis, 8 July 2008.

NII/CIO Briefing, Friendly Force Information (FFI) Attribute Based Access Control (ABAC) OPS Demo Information Briefing, Presented to STRIKE Steering Committee (SSC), 29 July 2008.

Allied Connectivity Team, Strike (COI) Steering Committee, 29 July 2008, Air Commodore Graham Wright.

Command and Control (C2) Portfolio Data Strategy Management, DRAFT, Configuration Management (CM) Plan v1.0.

Allied Connectivity Team, Strike (COI) Steering Committee, 29 July 2008, Mr. Tim Linderman, Strike COI Allied Connectivity Team Lead / USSTRATCOM JFCC-GSI/J32.

Authoritative C2 Data Status, August 21, 2008, JFCOM J8.

JFCC Global Strike, Strike Community of Interest Steering Committee, RDML Caldwell, 21 July 2008.

IED-D ICDT Battle Command, US Army Combined Arms Center, Mr. Robert Hartel, Battle Command Integration Directorate, 18 December 2007.

Acronyms and Abbreviations

ADS	Authoritative Data Source
AOR	Areas of Operation
ASA	Acquisition Shared Awareness
ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
ATO	Air Tasking Order
C2	Command and Control
C2ISF	C2 Information Sharing Network
CC/S/A	CoComs, Services and Agencies
CES	Core Enterprise Services
CIO	Chief Information Officer
CM	Configuration Management
COCOM	Combatant Command
COI	Community of Interest
CONOPS	Concepts of Operation
COP	Common Operational Picture (hopefully obsolete)
COTS	Commercial bought Off the Shelf System
CPM	Capability Portfolio Manager
CVT	Community Vocabulary Team
DDMS	DoD Discovery Metadata Specification
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry and Profile Registry
DL	Description Logics
DMZ	“Demilitarized Zone” a network device used to prevent unwanted penetration
DoD	Department of Defense
EDI	Electronic data interchange
ERP	Enterprise Resource Planning System
ESB	Enterprise Service Bus
FOA	Field Operating Activity
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GIS	Geographic Information System
HTML	Hyper Text Markup Language
IAT	Independent Assessment Team
IDA	Institute for Defense Analyses
IDEF	Integrated Definition

IEDM	Information Exchange Data Model
IOC	Initial Operating Capability
IPT	Integrated Product Team
IR	Information Resource
ISE	Information Sharing Environment
ISR	Intelligence, Surveillance, Reconnaissance
IT	Information Technology
JC3IEDM	Joint Command, Control, and Consultation Information Exchange Data Model
JCIDS	Joint Capabilities Integration and System Development
JCOM	Joint Forces Command
JTF	Joint Task Force
MA	Mission Area
MDE	Metadata Environment
MDR	Metadata Registry
MIP	Multilateral Interoperability Programme
NCDS	Net-Centric Data Strategy
NCES	Net-Centric Enterprise Services
NCO	Net-Centric Operations
NECC	Net-Enabled Command Capability
NGA	National Geospatial Agency
NGO	Non-Governmental Organizations
NII	Networks and Information Integration
NIPR	Non-Secure Internet Protocol Router Network
OASD	Assistant Secretary of Defense
OGC	Open Geospatial Consortium
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense
OTH	Over the Horizon
OWL	Web Ontology Language
PEO	Program Executive Officers
POAM	Plan of Action and Milestones
POC	Point of Contact
PoR	Program of Record
PPBE	Planning, Programming, Budgeting and Execution
PSA	Principal Staff Assistant
RDBMS	Relational Database Management System
ROI	Return on Investment
RSS	Really Simple Syndication
SIPR	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SQL	Structured Query Language
SSATF	Shared Situational Awareness Track Framework
TEMP	Test and Evaluation Master Plan
TTP	Tactics, Techniques and Procedures

UDDI	Universal Description, Discovery and Integration Protocol
UID	Unique Identifier
UJTL	Uniform Joint Task List
UML	Unified Modeling Language
VMF	Variable Message Format
WSDL	Web Service Definition Language
XML	Extensible Markup Language

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
November 2008	Study	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Independent Assessment Team Report on C2 Data	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Dawn Meyerriecks, Stan Davis, Jim Pipher, Priscilla Guthrie	5e. TASK NUMBER BC-1-2526
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBERI
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Paper P-4404

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
OASD (NII) 6000 Defense Pentagon Washington, Dc 20301-6000	OASD (NII)
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, unlimited distribution: 11 August 2009.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This Independent Assessment Team (IAT) was sponsored by ASD (NII) to provide C2 data policy and implementation guidance recommendations. The IAT'S recommendations are: 1) implement the DoD's Net-Centric Data Strategy for C2 using UCore and a redefined C2 Core, 2) grow C2 Core incrementally based on operational priorities, 3) define roles and responsibilities, 4) establish required C2 and enterprise governance (e.g., for CM, versioning), 5) increase focus on operations and tighten linkages between operators and developers, 6) plan for change – that is the benefit of a net-centric SOA.

15. SUBJECT TERMS

Data, C2 Data, C2 Data Strategy, NCDS (Net-Centric Data Strategy), C2 Core, C2 Data Sharing, C2 Information Sharing Framework, C2 Data Implementation.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mr. Ronald Pontius
Unclassified	Unclassified	Unclassified	Unlimited	95	19b. TELEPHONE NUMBER (Include Area Code) (703) 607-0670